SUMMIT ON INTEROPERABLE COMMUNICATIONS FOR PUBLIC SAFETY

June 26-27, 2003

Program Summary and Capabilities Survey Report

Sponsored by
The Department of Commerce
The National Institute of Standards and Technology
Office of Law Enforcement Standards

The Department of Justice
The National Institute of Justice
AGILE Program

The Department of Homeland Security
Science and Technology Directorate
SAFECOM

Version 1.02
Printed on:
9/17/2003 1:02:35 PM

Page	*Program/Organization*
4	AGILE
12	Association of Public-Safety Communications Officials -- International
13	Automated Regional Justice Information Systems
16	Bureau of Justice Assistance
19	San Diego Border Tactical Communications System
21	Capital Wireless Integrated Network
24	Center for Disease Control
25	Criminal Justice Information Services (Division)
27	Coast Guard National Distress & Response System Modernization Program Phase II (NDRSMP)
31	Communications for Coordinated Assistance and Response to Emergencies Alliance
34	Community Oriented Policing Services
38	Drug Enforcement Administration/National Drug Pointer Index Program
40	Department of Transportation - Intelligent Transportation System
43	Electronic Proving Grounds, Technology Transfer Program for ONDCP/CTAC
45	Federal Communications Commission/Public Safety & Private Wireless Division
46	Federal Chief Information Officers Council
47	Federal Law Enforcement Wireless Users' Group
48	Federal Wireless Users' Forum
49	Global Justice Information Sharing Initiative
51	Guard Net XXI
52	Homeland Security Standards Panel
53	Interagency Board for Equipment Standardization and Interoperability
54	International Association of Chiefs of Police
55	International Association of Fire Chiefs
56	Institute of Electrical and Electronics Engineers (IEEE), Committee 1512
59	Institute of Electrical and Electronics Engineers (IEEE), Committee 802
62	INTELINK Program
63	Integrated Wireless Network
67	Joint Tactical Radio System Joint Program Office
70	Major City Chiefs Association
71	Major County Sheriffs' Association
72	NASA's Earth Alert Program
76	National Association of State Chief Information Officers
78	The National Association of State Telecommunications Directors
79	National Criminal Justice Association
81	National Communications System
84	National Conference of States on Building Codes and Standards
89	National Drug Pointer Index (NDPIX)
90	National Emergency Management Association
91	National Fire Protection Association
92	National Governors Association (Center for Best Practices)
93	National Institute of Standards and Technology
96	National Law Enforcement and Corrections Technology Center
102	National Law Enforcement Telecommunication System
106	National Public Safety Telecommunications Council
108	Naval Research Laboratory / InfraLynx
112	National Sheriffs' Association
113	National Telecommunications and Information Administration Public Safety Program
115	Organization for the Advancement of Structured Information Standards
116	Office of Domestic Preparedness
118	Office of Law Enforcement Standards
124	Office of National Drug Control Policy / Counterdrug Technology Assessment Center

126 Office of National Preparedness
127 Oregon RAINS (Regional Alliance for Infrastructure and Network Security)
132 Partnership for Public Warning - All-Hazard Public Warning System
133 Public Safety Digital Radio Standard
139 Mobility for Emergency and Safety Applications
146 Public Safety Wireless Network (PSWN) Program
151 Regional Information Sharing Systems
155 Science and Technology Directorate
156 Wireless Public SAFEty Interoperable COMmunications (SAFECOM) Program
157 Strategic National Stockpile Program
159 Telecommunications Industry Association
160 Telecommunications Industry Association, TR-8 Mobile and Personal Private Radio Standards

Program/Organization:	**AGILE**
Full Name:	AGILE
Agencies:	Department of Justice, National Institute of Justice
Partnering Agencies / Orgs.:	NIST/OLES, National Law Enforcement and Corrections Technology Center (NLECTC), Bureau of Justice Assistance (BJA), Office of Domestic Preparedness (ODP), COPS, Office of National Preparedness (ONP-FEMA), SAFECOM (S&T Directorate, DHS), PSWN, NPSTC, NTFI
Web Page:	www.agileprogram.org
Contact Name:	Tom Coty
	Senior Program Manager for AGILE
Contact Phone:	202-514-7683
Contact Email:	cotyt@ojp.usdoj.gov

Current Products:

o PRACTITIONER OUTREACH
- Liaison with practitioners to establish user requirements for communications and interoperability, to provide tools for frequency band planning, system planning, and implementation, and to share lessons learned and best practices
- Funding the Support Office for the National Public Safety Telecommunications Council (NPSTC) and development of the 700-MHz Pre-coordination Data Base
- Funding and technical support to the NIJ's National Law Enforcement and Corrections Technology Centers
- Develop information media on interoperability issues, such as the video 'Why Can't We Talk?'

o ENGINEERING AND RESEARCH LABORATORY
- Provide test and evaluation studies of equipment that practitioners might use for communications and information technology
- Test interoperability of Project 25-compliant radio equipment and services
- Test technical performance of audio gateway switches, such as ACU-1000 and ICRI
- Test technical performance of Voice-over-IP (VoIP) applications, such as EFJohnson 2600 repeaters and ViperNet

o IMPLEMENTATION AND OPERATIONAL TEST BED
- Provide operational test bed to evaluate implementation and operation of interoperable equipment and solutions
- Evaluate audio interconnect systems use as a gateway between several agencies, such as ACU-1000 and ICRI

o RESEARCH AND DEVELOPMENT GRANTS
- Stimulate new technologies and solutions for interoperability through grants
- Fund Software Defined Radio (SDR) approaches for Public Safety applications
- Fund the development with ODP of the CapWIN System for public safety and transportation mobile data in the Washington, DC, Metro area.

o SPECIFICATIONS AND STANDARDS DEVELOPMENT
- Support development of user requirements, specifications, and standards for interoperable communications equipment and information sharing
- Provide user requirements and specifications to Project MESA
- Provide technical assistance on standards development to Project 25
- Provide technical assistance on specifications to GLOBAL Program

o ELECTED AND APPOINTED OFFICIALS OUTREACH

Program/Organization:	**AGILE**
	- Provide education for elected and appointed officials through forums such as the National Task Force on Interoperability o CONVENIENT ACCESS TO INFORMATION RESOURCES - Reports, resources, and discussions on grants, research and development, and standards through the AGILE website: www.agileprogram.org - Guides (such as the Antenna System Guide), briefings (such as the Communications Interoperability Technology Brief), and analysis (such as the Wireless Interoperability Analysis) of interoperable solutions through a CD-ROM Interoperability Toolkit - Standards for communications and information sharing (such as the CD-ROM Project 25 --- The TIA-published 102 Series Documents with the current TIA-102 approved overview documents and technical standards on the Project 25 General System Model Interfaces)
Planned Products:	Continued efforts to provide products that meet the interoperability needs of Public Safety agencies through equipment test and evaluation, research and development, outreach and education, and standards.
Additional Information:	
Program Goals:	Note: The emphasis in AGILE is on the technical efforts and outreach for public safety and law enforcement communications, including the following: 1. Providing technical support for standards development (e.g., Project 25 standards and specifications) 2. R&D efforts to develop technology solutions, provide technical analyses, reports, and guides 3. Testing of telecommunications and IT technology applications (e.g., testing the ACU-1000 switches) 4. Institutionalize the issue of communications interoperability along with its best practices and solutions for public safety and elected and appointed leaders of the state and local community

Sectors Addressed:			
☑ *Law Enforcement*	☑ *Corrections*	☑ *EMS*	☑ *Military*
☑ *Courts*	☑ *Probat./Parole*	☑ *Emerg. Manag.*	☐ *Other*
☑ *Public Defender*	☑ *Fire Protection*	☑ *Transportation*	
☑ *Prosecution*	☑ *Public Works*	☑ *Utlities*	

Functional Capabilities:

Wireless Voice

☑ Ability to initiate wireless voice communications by requiring the user to only enter (on his/her radio) a user identification which authenticates and validates the user, registers and sets talk groups/capabilities for the user, and completes all radio network administration for the user's voice communications with other members of the user's agency/jurisdiction and with other agencies/jurisdictions, as authorized.

Program efforts associated with Standardization (through direct technical support to Project 25, Project MESA, NPSTC working groups, and the Software Defined Radio Forum), R&D (for example through grants facilitating software defined radio development), test and evaluation of prospective standardized approaches (before they are offered to standards committees), and test and evaluation of standard products to determine the degree of interoperability among them.

Wireless Voice

☑ Ability for users to transparently communicate, as authorized, with other members of the agency/jurisdiction on a unit-to-group (one-to-many) basis and a unit-to-unit (one-to-one) basis.

Program efforts associated with Standardization (through direct technical support to Project 25, Project MESA, NPSTC working groups, and the Software Defined Radio Forum), R&D (for example through grants facilitating software defined radio development), test and evaluation of prospective standardized approaches (before they are offered to standards committees), and test and evaluation of standard products to determine the degree of interoperability among them.

Wireless Voice

☑ Ability of the agency/jurisdiction to administer the priority for voice communications of particular users and particular applications (such as task force operations, incidents, etc.).

Program efforts associated with Standardization (through direct technical support to Project 25, Project MESA, NPSTC working groups, and the Software Defined Radio Forum), R&D (for example through grants facilitating software defined radio development), test and evaluation of prospective standardized approaches (before they are offered to standards committees), and test and evaluation of standard products to determine the degree of interoperability among them.

Wireless Voice

☑ Ability to communicate an emergency voice message and/or signal which has priority over other voice communications.

Program efforts associated with Standardization (through direct technical support to Project 25, Project MESA, NPSTC working groups, and the Software Defined Radio Forum), R&D (for example through grants facilitating software defined radio development), test and evaluation of prospective standardized approaches (before they are offered to standards committees), and test and evaluation of standard products to determine the degree of interoperability among them.

Wireless Voice

☑ Ability to have secure voice communications.

Program efforts associated with Standardization (through direct technical support to Project 25, Project MESA, NPSTC working groups, and the Software Defined Radio Forum), R&D (for example through grants facilitating software defined radio development), test and evaluation of prospective standardized approaches (before they are offered to standards committees), and test and evaluation of standard products to determine the degree of interoperability among them.

Wireless Voice

☑ Ability for users to transparently communicate, as authorized, among multiple agencies/jurisdictions some of which may use different technologies, infrastructures and/or frequency bands.

Program efforts associated with Standardization (through direct technical support to Project 25, Project MESA, NPSTC working groups, and the Software Defined Radio Forum), R&D (for example through grants facilitating software defined radio development), test and evaluation of prospective standardized approaches (before they are offered to standards committees), test and evaluation of standard products to determine the degree of interoperability among them, and test and evaluation of commercially available and emerging interoperability devices.

Wireless Voice

☑ Ability to remotely access a user's agency/jurisdiction voice communications infrastructure when the user roams outside the radio coverage area of the user's agency/jurisdiction wireless infrastructure.

Program efforts associated with Standardization (through direct technical support to Project 25, Project MESA, NPSTC working groups, and the Software Defined Radio Forum), R&D (for example through grants facilitating software defined radio development), test and evaluation of prospective standardized approaches (before they are offered to standards committees), test and evaluation of standard products to determine the degree of interoperability among them, and test and evaluation of commercially available and emerging interoperability devices.

Wireless Voice

☑ Ability to effectively initiate and sustain flexible and dynamic system administration (includes administration of talk groups, emergency alerts, networks, and channels for mutual aid).

Program efforts associated with Standardization (through direct technical support to Project 25, Project MESA, NPSTC working groups, and the Software Defined Radio Forum), R&D (for example through grants facilitating software defined radio development), test and evaluation of prospective standardized approaches (before they are offered to standards committees), and test and evaluation of standard products to determine the degree of interoperability among them.

Wireless Voice

☑ Ability to sustain highly reliable system performance across interconnected systems (including tolerance to individual system failures, redundant coverage from adjacent sites, resistance to impact of catastrophic events, etc).

Program efforts associated with Standardization (through direct technical support to Project 25, Project MESA, NPSTC working groups, and the Software Defined Radio Forum), R&D (for example through grants facilitating software defined radio development), test and evaluation of prospective standardized approaches (before they are offered to standards committees), and test and evaluation of standard products to determine the degree of interoperability among them.

Wireless Voice

☑ Ability to remotely (over-the-air) reprogram a user's radios and/or modify a user's encryption keys and/or modify a radio's waveforms.

Program efforts associated with Standardization (through direct technical support to Project 25, Project MESA, NPSTC working groups, and the Software Defined Radio Forum), R&D (for example through grants facilitating software defined radio development), test and evaluation of prospective standardized approaches (before they are offered to standards committees), and test and evaluation of standard products to determine the degree of interoperability among them.

Wireless Voice

☑ Ability to provide state-wide (county-wide) signal coverage to vehicular/mobile radios on highways and at street level for state (county) agencies, to provide city-wide signal coverage to portable/handheld radios on the street and within buildings for city agencies, and to provide direct communications between user radios when there is no wireless infrastructure to support communications (such in some rural areas, underground parking garages, and inside some buildings).

Program efforts associated with Standardization (through direct technical support to Project 25, Project MESA, NPSTC working groups, and the Software Defined Radio Forum), R&D (for example through grants facilitating software defined radio development), test and evaluation of prospective standardized approaches (before they are offered to standards committees), test and evaluation of standard products to determine the degree of interoperability among them, and test and evaluation of commercially available and emerging interoperability devices.

Wireless Data

☑ Ability to initiate wireless data communications by requiring the user to only enter (on his/her data terminal/radio) a user identification which authenticates and validates the user, registers and sets data resource capabilities for the user, and completes all radio network administration for the user's data communications with other members of the user's agency/jurisdiction and with other agencies/jurisdictions, as authorized.

Program efforts associated with Standardization (through direct technical support to Project 25, Project MESA, NPSTC working groups, and the Software Defined Radio Forum), R&D (for example through grants facilitating software defined radio development), test and evaluation of prospective standardized approaches (before they are offered to standards committees), and test and evaluation of standard products to determine the degree of interoperability among them.

Wireless Data

☑ Ability of users to quickly and transparently establish on-scene wireless data networks that function among data terminals located in on-scene vehicles and among data terminal carried by users into buildings, etc.

Program efforts associated with Standardization (through direct technical support to Project 25, Project MESA, NPSTC working groups, and the Software Defined Radio Forum), R&D (for example through grants facilitating software defined radio development), test and evaluation of prospective standardized approaches (before they are offered to standards committees), and test and evaluation of standard products to determine the degree of interoperability among them.

Wireless Data

☑ Ability of on-scene personnel to transparently exchange, as authorized, text, image, and/or video data with other on-site personnel, dispatchers, data resources, etc.

Program efforts associated with Standardization (through direct technical support to Project 25, Project MESA, NPSTC working groups, and the Software Defined Radio Forum), R&D (for example through grants facilitating software defined radio development), test and evaluation of prospective standardized approaches (before they are offered to standards committees), and test and evaluation of standard products to determine the degree of interoperability among them.

Wireless Data

☑ Ability to protect the privacy of particular information according to applicable laws and statutes so that it can be accessed only by authorized personnel and data terminals.

Program efforts associated with Standardization (through direct technical support to Project 25, Project MESA, NPSTC working groups, and the Software Defined Radio Forum), R&D (for example through grants facilitating software defined radio development), test and evaluation of prospective standardized approaches (before they are offered to standards committees), and test and evaluation of standard products to determine the degree of interoperability among them.

Wireless Data

☑ Ability to ensure secure exchange of information.

Program efforts associated with Standardization (through direct technical support to Project 25, Project MESA, NPSTC working groups, and the Software Defined Radio Forum), R&D (for example through grants facilitating software defined radio development), test and evaluation of prospective standardized approaches (before they are offered to standards committees), and test and evaluation of standard products to determine the degree of interoperability among them.

Wireless Data

☑ Capability of high speed data transfer to allow fast exchange of text, image, and streaming video information.

Program efforts associated with Standardization (through direct technical support to Project 25, Project MESA, NPSTC working groups, and the Software Defined Radio Forum), R&D (for example through grants facilitating software defined radio development), test and evaluation of prospective standardized approaches (before they are offered to standards committees), and test and evaluation of standard products to determine the degree of interoperability among them.

Wireless Data

☑ Ability of transparent on-scene system access to multiple information systems regardless of differing data base system architectures and data formats.

Program efforts associated with Standardization (through direct technical support to Project 25, Project MESA, NPSTC working groups, and the Software Defined Radio Forum), R&D (for example through grants facilitating software defined radio development), test and evaluation of prospective standardized approaches (before they are offered to standards committees), and test and evaluation of standard products to determine the degree of interoperability among them.

Wireless Data

☑ Ability to remotely access a user's agency/jurisdiction data communications infrastructure when the user roams outside the radio coverage area of the user's agency/jurisdiction infrastructure.

Program efforts associated with Standardization (through direct technical support to Project 25, Project MESA, NPSTC working groups, and the Software Defined Radio Forum), R&D (for example through grants facilitating software defined radio development), test and evaluation of prospective standardized approaches (before they are offered to standards committees), test and evaluation of standard products to determine the degree of interoperability among them, and test and evaluation of commercially available and emerging interoperability devices.

Program/Organization:	**AGILE**

Wireless Data

☑ Reliable system operational performance (including fault tolerant to individual system failures, redundant coverage from adjacent sites, full service during routine maintenance, and resistant to impact of catastrophic events).	Program efforts associated with Standardization (through direct technical support to Project 25, Project MESA, NPSTC working groups, and the Software Defined Radio Forum), R&D (for example through grants facilitating software defined radio development), test and evaluation of prospective standardized approaches (before they are offered to standards committees), and test and evaluation of standard products to determine the degree of interoperability among them.

Wireless Data

☑ Flexible and dynamic system administration (includes administration of on-scene wireless data networks).	Program efforts associated with Standardization (through direct technical support to Project 25, Project MESA, NPSTC working groups, and the Software Defined Radio Forum), R&D (for example through grants facilitating software defined radio development), test and evaluation of prospective standardized approaches (before they are offered to standards committees), and test and evaluation of standard products to determine the degree of interoperability among them.

Information Systems

☑ Ability to effectively and efficiently exchange data between agencies/jurisdictions, e.g., by employing common data representation structures and exchange formats and protocols.	Program efforts associated with Standardization (through direct technical support to GLOBAL Justice Information Sharing Initiative Standards Committees, and in particular to the standardization of XML implementation approaches, XML data element dictionary, XML Schema, and Information Sharing Registry).

Information Systems

☑ Ability to rapidly access subject information at critical decision points from both field and base locations, including but not limited to information regarding identification (photos, fingerprints, etc.) and activity (criminal history, wants/warrants, reporting/contact history, etc.).	Program efforts associated with Standardization (through direct technical support to GLOBAL Justice Information Sharing Initiative Standards Committees, Project 25, and Project MESA.

Information Systems

☑ Ability to enter information once, then share and reuse that information among all entities that require it.	Program efforts associated with Standardization (through direct technical support to GLOBAL Justice Information Sharing Initiative Standards Committees, and in particular to the standardization of XML implementation approaches, XML data element dictionary, XML Schema, and Information Sharing Registry, and to the standardization of architectural frameworks, and information sharing processes and procedures).

Information Systems

☑ Ability to query/access multiple data sources using one request that is routed to multiple entities simultaneously.	Program efforts associated with Standardization (through direct technical support to GLOBAL Justice Information Sharing Initiative Standards Committees, and in particular to the standardization of XML implementation approaches, XML data element dictionary, XML Schema, and Information Sharing Registry, and to the standardization of architectural frameworks, and information sharing processes and procedures).

Information Systems

☑ Capability of standardized security, including functions and features that can be used to satisfy reasonable security requirements of any entity within a broader security framework.	Program efforts associated with Standardization (through direct technical support to GLOBAL Justice Information Sharing Initiative Standards Committees, and in particular to the standardization of XML implementation approaches, XML data element dictionary, XML Schema, and Information Sharing Registry, and to the standardization of architectural frameworks, and information sharing processes and procedures).

Program/Organization:	**AGILE**

Information Systems

☑ Ability to exchange information with Computer-Aided Dispatch (CAD) systems.	Program efforts associated with Standardization (through direct technical support to GLOBAL Justice Information Sharing Initiative Standards Committees, IEEE 1512 Standards Committee, Project 25 and Project MESA).

Information Systems

☑ Capability of field photo scanning and image file distribution.	Program efforts associated with Standardization (through direct technical support to GLOBAL, Project 25, Project MESA, NPSTC working groups, and the Software Defined Radio Forum), R&D (for example through grants facilitating software defined radio development), test and evaluation of prospective standardized approaches (before they are offered to standards committees), test and evaluation of standard products to determine the degree of interoperability among them, and test and evaluation of commercially available and emerging interoperability devices.

Information Systems

☑ Ability to have near-real-time distribution of text messages to multiple organizations responding to a large event.	Program efforts associated with Standardization (through direct technical support to GLOBAL Justice Information Sharing Initiative Standards Committees, IEEE 1512 Standards Committee, Project 25 and Project MESA).

Information Systems

☑ Ability to access information related to hazardous materials, water sources, floor and building plans, utility maps, weather forecasts, topographic terrain, and other background data that may influence how public safety practitioners approach or conduct operations at an incident.	Program efforts associated with Standardization (through direct technical support to GLOBAL Justice Information Sharing Initiative Standards Committees and working groups of the InterAgency Board for Equipment Standardization and Interoperability (IAB).

Information Systems

☑ Ability to access medical/treatment records (both those required to ensure proper treatment of incident victims and/or prisoners and those records obtained under warrant).	Program efforts associated with Standardization (through direct technical support to GLOBAL Justice Information Sharing Initiative Standards Committees and working groups of the InterAgency Board for Equipment Standardization and Interoperability (IAB).

Information Systems

☑ Ability to access information regarding pending investigation/litigation of a particular subject.	Program efforts associated with Standardization (through direct technical support to GLOBAL Justice Information Sharing Initiative Standards Committees, and in particular to the standardization of XML implementation approaches, XML data element dictionary, XML Schema, and Information Sharing Registry, and to the standardization of architectural frameworks, and information sharing processes and procedures).

Information Systems

☑ Ability to access court scheduling information.	Program efforts associated with Standardization (through direct technical support to GLOBAL Justice Information Sharing Initiative Standards Committees, and in particular to the standardization of XML implementation approaches, XML data element dictionary, XML Schema, and Information Sharing Registry, and to the standardization of architectural frameworks, and information sharing processes and procedures).

Information Systems

☑ Ability to automatically link disposition data with charge data on subject RAP sheet/CCH information.	Program efforts associated with Standardization (through direct technical support to GLOBAL Justice Information Sharing Initiative Standards Committees, and in particular to the standardization of XML implementation approaches, XML data element dictionary, XML Schema, and Information Sharing Registry, and to the standardization of architectural frameworks, and information sharing processes and procedures).

Program/Organization:	**AGILE**

Information Systems

☑ Capability of automatic dissemination of disposition data to appropriate local, state, and federal agencies/databases.	Program efforts associated with Standardization (through direct technical support to GLOBAL Justice Information Sharing Initiative Standards Committees, and in particular to the standardization of XML implementation approaches, XML data element dictionary, XML Schema, and Information Sharing Registry, and to the standardization of architectural frameworks, and information sharing processes and procedures).

Information Systems

☑ Ability to access current resource data (including personnel, equipment, materials, etc.) of multiple agencies/jurisdictions responding to a multi-agency/jurisdictional event by authorized users in the respective agencies/jurisdictions.	Program efforts associated with Standardization (through direct technical support to GLOBAL Justice Information Sharing Initiative Standards Committees, and in particular to the standardization of XML implementation approaches, XML data element dictionary, XML Schema, and Information Sharing Registry, and to the standardization of architectural frameworks, and information sharing processes and procedures).

Program/Organization:	**APCO, International, Inc.**
Full Name:	Association of Public-Safety Communications Officials -- International
Agencies:	International Association
Partnering Agencies / Orgs.:	State and local Public Safety organizations that use, manage, operate, maintain, and supply public safety communications
Web Page:	http://www.apcointl.org/
Contact Name:	Vincent Stile
	Acting President
Contact Phone:	631-852-6431 or 888-APCO 9-1-1
Contact Email:	stilev@apco911.org

Current Products:	o Project 25 development o Advocate to free 700 MHz for Public Safety o Project 34 (Project MESA) development o Project 39 -- Interference to 800 MHz Public Safety Radio Systems issues and solutions o Frequency coordination
Planned Products:	
Additional Information:	APCO International, Washington, DC, Office 1725 DeSales Washington, DC 20036 202-833-2700 Also: 202-833-9600 APCO International, Inc. 351 N. Williamson Blvd Daytona Beach, FL 32114-1112 1-888-APCO-9-1-1 Also 386-322-2500
Program Goals:	o To influence Public Safety communications decisions of government and industry o To foster development and use of technology APCO International provides membership services to the sectors checked below in the form of training, operational information assisstance, public safety frequency coordination, special on-site agency assistance as related to public safety communications, and is the public safety advocate to the FCC and Congress in matters related to public safety communications.

Sectors Addressed:	☑ ***Law Enforcement***	☑ ***Corrections***	☑ ***EMS***	☐ ***Military***
	☐ ***Courts***	☑ ***Probat./Parole***	☑ ***Emerg. Manag.***	☐ ***Other***
	☐ ***Public Defender***	☑ ***Fire Protection***	☑ ***Transportation***	
	☐ ***Prosecution***	☑ ***Public Works***	☐ ***Utlities***	

Program/Organization:	**ARJIS**
Full Name:	Automated Regional Justice Information Systems
Agencies:	San Diego Police Department
Partnering Agencies / Orgs.:	San Diego law-enforcement, courts, and corrections, namely: The Police & Sheriff's Departments of San Diego, Chula Vista, La Mesa, Coronado, Oceanside, El Cajon, Escondido, National City, Del Mar, San Marcos, Encinitas, Santee, Imperial Beach, Solana Beach, Lemon Grove, Vista, and Poway
Web Page:	http://www.arjis.org
Contact Name:	Pam Scanlon
Contact Phone:	619-533-4204
Contact Email:	pscanlon@arjis.org
Current Products:	Web-based access to criminal justice information in the San Diego region. EDIS is the Emergency Digital Information Service, which delivers official information about emergencies and disasters to the public and the news media in California.
Planned Products:	
Additional Information:	
Program Goals:	The Automated Regional Justice Information System (ARJIS) is a complex criminal justice enterprise network utilized by 38 local, state, and federal agencies in the San Diego region. ARJIS is chartered with supporting a regional web-based enterprise network that utilizes technical and operational standards to build interfaces to all criminal justice systems in the region. The ARJISNet secure intranet contains data on the region's crime cases, arrests, citations, field interviews, traffic accidents, fraudulent documents, photographs, gang information, and stolen property.

Sectors Addressed:	☑ ***Law Enforcement***	☐ ***Corrections***	☑ ***EMS***	☐ ***Military***
	☑ ***Courts***	☑ ***Probat./Parole***	☑ ***Emerg. Manag.***	☐ ***Other***
	☑ ***Public Defender***	☑ ***Fire Protection***	☑ ***Transportation***	
	☑ ***Prosecution***	☑ ***Public Works***	☐ ***Utlities***	

Functional Capabilities:

Wireless Voice

☑ Ability to initiate wireless voice communications by requiring the user to only enter (on his/her radio) a user identification which authenticates and validates the user, registers and sets talk groups/capabilities for the user, and completes all radio network administration for the user's voice communications with other members of the user's agency/jurisdiction and with other	800 MHz radio system with over 127 agencies participating - establish talk groups/identification based on a regional template.

agencies/jurisdictions, as authorized.

Wireless Voice

☑ Ability for users to transparently communicate, as authorized, with other members of the agency/jurisdiction on a unit-to-group (one-to-many) basis and a unit-to-unit (one-to-one) basis.	Part of the RCS capabilities

Wireless Voice

☑ Ability of the agency/jurisdiction to administer the priority for voice communications of particular users and particular applications (such as task force operations, incidents, etc.).	Part of the RCS capabilities

Wireless Voice

☑ Ability to communicate an emergency voice message and/or signal which has priority over other voice communications.	Part of the RCS capabilities

Wireless Voice

☑ Ability to have secure voice communications.	Part of the RCS capabilities

Wireless Voice

☑ Ability for users to transparently communicate, as authorized, among multiple agencies/jurisdictions some of which may use different technologies, infrastructures and/or frequency bands.	Part of the BORTAC System capabilities

Wireless Voice

☑ Ability to effectively initiate and sustain flexible and dynamic system administration (includes administration of talk groups, emergency alerts, networks, and channels for mutual aid).	Part of the RCS capabilities

Wireless Voice

☑ Ability to sustain highly reliable system performance across interconnected systems (including tolerance to individual system failures, redundant coverage from adjacent sites, resistance to impact of catastrophic events, etc).	Part of the RCS and BORTAC System capabilities

Information Systems

☑ Ability to effectively and efficiently exchange data between agencies/jurisdictions, e.g., by employing common data representation structures and exchange formats and protocols.	Standardized reporting and incidents for 50 agencies and all jurisdictions inputting data. Justice XML data exchange standards are utilized for all interfaces.

Information Systems

☑ Ability to rapidly access subject information at critical decision points from both field and base locations, including but not limited to information regarding identification (photos, fingerprints, etc.) and activity (criminal history, wants/warrants, reporting/contact history, etc.).	Photos connected statewide via Cal-Photo, Wants/Warrants, and other data from 15 disparate databases linked through a Global Query function accessible in the field and office

Program/Organization: **ARJIS**

	Information Systems	
☑	Ability to enter information once, then share and reuse that information among all entities that require it.	Single entry completed for law enforcement functions, jail bookings, and court citations – in process for DA, Probatin, 290-sex registration, and state databases
	Information Systems	
☑	Ability to query/access multiple data sources using one request that is routed to multiple entities simultaneously.	Global Query (web based application) hits 15 disparate databases with a single query
	Information Systems	
☑	Capability of standardized security, including functions and features that can be used to satisfy reasonable security requirements of any entity within a broader security framework.	All 50 ARJIS agencies are linked together via a private secure intranet – ARJISNET – and utilize LDAP security center for authentication
	Information Systems	
☑	Ability to exchange information with Computer-Aided Dispatch (CAD) systems.	CAD data is shipped from San Diego Police for mapping and statistics – a programmatic interface is being developed to embed the Global Query function into each individual agency's CAD system
	Information Systems	
☑	Capability of field photo scanning and image file distribution.	Booking photos are distributed via hand helds to the field and via short range wireless if available. No photo scanning from the field at this time.
	Information Systems	
☑	Ability to access information related to hazardous materials, water sources, floor and building plans, utility maps, weather forecasts, topographic terrain, and other background data that may influence how public safety practitioners approach or conduct operations at an incident.	Most data is maintained in separate agency CAD systems
	Information Systems	
☑	Ability to access court scheduling information.	On-line access to all agencies
	Information Systems	
☑	Capability of automatic dissemination of disposition data to appropriate local, state, and federal agencies/databases.	Accessible to all 50 participating agencies on-line via a name or case-number query

Program/Organization:	**BJA**
Full Name:	Bureau of Justice Assistance
Agencies:	Information Technology Policy Office
Partnering Agencies / Orgs.:	1. Global Justice Information Sharing Initiative (GLOBAL) 2. Industry Working Group / IJIS Institute 3. Other OJP Organizations (NIJ BJS, etc.) 4. Various state and local practitioner based standards groups
Web Page:	http://www.ojp.usdoj.gov/BJA/
Contact Name:	Patrick McCreary
	Program Manager
Contact Phone:	202-616-0532
Contact Email:	mccrearj@ojp.usdoj.gov
Current Products:	1. Justice XML Data Model/Data Dictionary 2. IT initiatives Website (http://www.it.ojp.gov) 3. Justice Standards Clearinghouse 4. Justice Information Exchange Model Tool (JIEM) 5. Justice Information Privacy Guideline 6. Security primer for justice practitioners
Planned Products:	1. XML Registry/Repository
Additional Information:	Grant programs support the following initiatives: 1. functional standards for law enforcement RMS and CAD systems (LEITS Council) 2. NASCIO Enterprise Architecture Toolkit 3. Integrated Justice Information Sharing (IJIS) Institute 4. technical assistance and training (SEARCH) 5. functional standards for court case management systems, corrections, and probation/parole 6. emerging technology seminars (IWG) 7. capability assessment toolkit (CTG) 8. performance measures (UNO) 9. NGA Justice IT Integration Projects Richard Nedelkoff, BJA Director Other BJA contacts: Dick Ward, Deputy Director J. Patrick McCreary, Sr. Policy Advisor 202-616-0532 mccrearj@ojp.usdoj.gov Bob Greeves, Policy Advisor 202-305-9317 greevesr@ojp.usdoj.gov Ken Gill, Technology Advisor 202-514-3719 gillk@ojp.usdoj.gov Bureau of Justice Assistance Office of Justice Programs U.S. Department of Justice 810 Seventh Street NW Washington, DC 20531 http://www.it.ojp.gov

Program/Organization:	**BJA**
Program Goals:	1. Strategic Planning and Governance 2. Standards, Infrastructure, and Enterprise Architecture 3. Privacy and Information Quality 4. Security

Sectors Addressed:	☑ *Law Enforcement*	☑ *Corrections*	☐ *EMS*	☐ *Military*
	☑ *Courts*	☑ *Probat./Parole*	☐ *Emerg. Manag.*	☐ *Other*
	☑ *Public Defender*	☐ *Fire Protection*	☐ *Transportation*	
	☑ *Prosecution*	☐ *Public Works*	☐ *Utlities*	

Functional Capabilities:

	Information Systems	
☑	Ability to effectively and efficiently exchange data between agencies/jurisdictions, e.g., by employing common data representation structures and exchange formats and protocols.	Supporting the development of the Justice XML Data Model and other data exchange standards such as the Justice Information Exchange Model.
	Information Systems	
☑	Ability to rapidly access subject information at critical decision points from both field and base locations, including but not limited to information regarding identification (photos, fingerprints, etc.) and activity (criminal history, wants/warrants, reporting/contact history, etc.).	Supporting multiple state implementations of integrated justice information systems through grants via the National Governor's Association.
	Information Systems	
☑	Ability to enter information once, then share and reuse that information among all entities that require it.	Supporting multiple state implementations of integrated justice information systems through grants via the National Governor's Association.
	Information Systems	
☑	Ability to query/access multiple data sources using one request that is routed to multiple entities simultaneously.	Supporting multi-jurisdictional criminal intelligence information sharing via six Regional Information Sharing Centers (RISS) and MATRIX.
	Information Systems	
☑	Capability of standardized security, including functions and features that can be used to satisfy reasonable security requirements of any entity within a broader security framework.	Supporting the Global Systems Security Compatibility Task Force.
	Information Systems	
☑	Ability to exchange information with Computer-Aided Dispatch (CAD) systems.	Supporting the Law Enforcement Information Technology Standards Council efforts to develop functional standards for CAD and RMS systems. Coordinate funding for multiple CAD/RMS implementations.

Program/Organization:	**BJA**

Information Systems

☑ Ability to access information related to hazardous materials, water sources, floor and building plans, utility maps, weather forecasts, topographic terrain, and other background data that may influence how public safety practitioners approach or conduct operations at an incident.	Supporting efforts by the IACP to establish standards for incident command systems.

Information Systems

☑ Ability to access medical/treatment records (both those required to ensure proper treatment of incident victims and/or prisoners and those records obtained under warrant).	Supporting the State Correctional Directors in the development of performance standards for managing health information.

Information Systems

☑ Ability to access information regarding pending investigation/litigation of a particular subject.	Supporting the development of model policies for access to electronic records associated with criminal investigations/litigation.

Information Systems

☑ Ability to access court scheduling information.	Supporting the National Center for State Courts, Conference of State Court Administrators, and the National Association of Court Managers through various initiatives.

Information Systems

☑ Ability to automatically link disposition data with charge data on subject RAP sheet/CCH information.	Supporting disposition linkage to criminal history records through the national criminal history records improvement program.

Information Systems

☑ Capability of automatic dissemination of disposition data to appropriate local, state, and federal agencies/databases.	Supporting the criminal records improvement program through the National Law Enforcement Telecommunications System to the FBI NCIC.

Program/Organization:	**BORTAC**
Full Name:	San Diego Border Tactical Communications System
Agencies:	DoJ, NIJ
Partnering Agencies / Orgs.:	U.S. Office of National Drug Policy (ONDCP), Counter Drug Technology Assessment Center (CTAC), the U.S. Navy, DOJ, and San Diego law-enforcement and public-safety agencies. Also: California Highway patrol, San Diego Police Department, San Diego Sheriff's Department, Chula Vista Police Department, Naval Base Security, Navy Investigative Service, Navy Fire Department, U.S. Coast Guard, U.S. Border Patrol, FBI, DEA, U.S. Customs Service
Web Page:	http://www.techcourt.com/law/news-0001.htm
Contact Name:	Robert J. Waldron
Contact Phone:	888-548-1618
Contact Email:	waldron@law-west.org
Current Products:	1. BORTAC (San Diego) A computer patch that translates modulation schemes to connect disparate radio communication systems among various LE and public-safety agencies.
Planned Products:	o BORTAC II (Imperial Valley)
Additional Information:	Additional contact: Chris Aldridge 888/656-2782 cdaldri@brtc.nlectc.org or brtcchrisa@aol.com
Program Goals:	Real-time, unencrypted, voice-communication interoperability among 12 Federal, state, and local law-enforcement and public-safety agencies with the use of commercial off-the-shelf radio and software components.

Sectors Addressed:				
☑ ***Law Enforcement***	☐ ***Corrections***	☑ ***EMS***	☐ ***Military***
☐ ***Courts***	☐ ***Probat./Parole***	☐ ***Emerg. Manag.***	☐ ***Other***
☐ ***Public Defender***	☑ ***Fire Protection***	☐ ***Transportation***	
☐ ***Prosecution***	☐ ***Public Works***	☐ ***Utlities***	

Functional Capabilities:

Wireless Voice

☑ Ability for users to transparently communicate, as authorized, with other members of the agency/jurisdiction on a unit-to-group (one-to-many) basis and a unit-to-unit (one-to-one) basis.	Agencies need to coordinate the setup of communications and once the setup is established, then the users can communicate transparently.

Program/Organization:	**BORTAC**

Wireless Voice

☑ Ability for users to transparently communicate, as authorized, among multiple agencies/jurisdictions some of which may use different technologies, infrastructures and/or frequency bands.	The system allows users from all bands, trunked and non-trunked, to interoperate once the communications are enabled. The normal situation is for the agencies to be separate until they decide to join communication link.

Program/Organization:	**CapWIN**
Full Name:	Capital Wireless Integrated Network
Agencies:	Capital Wireless Integrated Network
Partnering Agencies / Orgs.:	Maryland State Highway Admin., Virginia Dept of Transportation, U.S. DoT (FHWA), U.S. DoJ (ODP, OJP, NIJ/OST), PSWN (Public Safety Wireless Network), and the Univ. of Maryland.
Web Page:	http://www.capwinproject.com/
Contact Name:	George Ake
	Program Director, University of Maryland
Contact Phone:	301-614-3701
Contact Email:	gake@capwin.org
Current Products:	1. Equipped law-enforcement vehicles in the CapWIN area can communicate with text. 2. Maryland Board of Public Works awarded the CapWIN Systems Integrator contract.
Planned Products:	A model for integrated wireless computing among other public safety and transportation communities in the United States.
Additional Information:	gake@wam.umd.edu
Program Goals:	1. To develop an integrated mobile wireless network infrastructure 2. To develop a wireless network that provides critical information to public safety and transportation officials regarding life-threatening situations (HAZ-MAT, CNB/WMD, traffic stops, wanted persons, etc.) 3. To develop the requirements for future mobile data applications for transportation and public safety

Sectors Addressed:	☑ ***Law Enforcement***	☐ ***Corrections***	☑ ***EMS***	☐ ***Military***
	☐ ***Courts***	☐ ***Probat./Parole***	☑ ***Emerg. Manag.***	☐ ***Other***
	☐ ***Public Defender***	☑ ***Fire Protection***	☑ ***Transportation***	
	☑ ***Prosecution***	☑ ***Public Works***	☐ ***Utlities***	

Functional Capabilities:

Wireless Data

☑ Ability to initiate wireless data communications by requiring the user to only enter (on his/her data terminal/radio) a user identification which authenticates and validates the user, registers and sets data resource capabilities for the user, and completes all radio network administration for the user's data communications with other members of the user's agency/jurisdiction and with other agencies/jurisdictions, as authorized.

Authorization/authentication is handled by a combination of LDAP/RDBMS and VPN software which allows secure data communications and access to authorized resources only.

Program/Organization:	**CapWIN**

Wireless Data

☑ Ability of users to quickly and transparently establish on-scene wireless data networks that function among data terminals located in on-scene vehicles and among data terminal carried by users into buildings, etc.	CapWIN does not allow for the creation of "networks" per se but does allow for the coordination of resources and communication using its "incident management" framework.

Wireless Data

☑ Ability of on-scene personnel to transparently exchange, as authorized, text, image, and/or video data with other on-site personnel, dispatchers, data resources, etc.	Text, image data, and video are all possible and supported by the system. Video is not practical at this time due to limited bandwidth of most end-users.

Wireless Data

☑ Ability to protect the privacy of particular information according to applicable laws and statutes so that it can be accessed only by authorized personnel and data terminals.	The CapWIN system protects all information stored on the system from "end-to-end".

Wireless Data

☑ Ability to ensure secure exchange of information.	CapWIN supports numerous encryption methods including 3DES and FIPS 140-2. Encryption for all data transfer is "end-to-end".

Wireless Data

☑ Capability of high speed data transfer to allow fast exchange of text, image, and streaming video information.	The system is capable of handling this, however, there is currently no high-speed public safety data network available for the Capital area.

Wireless Data

☑ Ability of transparent on-scene system access to multiple information systems regardless of differing data base system architectures and data formats.	This is the heart of the CapWIN query subsystem. It allows seamless access to several back-end data sources. This is accomplished though a combination of Templar Corporation's Informant product, IBM's MQseries and XML data transfer.

Wireless Data

☑ Reliable system operational performance (including fault tolerant to individual system failures, redundant coverage from adjacent sites, full service during routine maintenance, and resistant to impact of catastrophic events).	The CapWIN system is fully redundant as to system hardware (clustering, dual power, etc.), software (HACMP, load-balancing, etc.), and communications (redundant communications links and hardware configurations). A fully redundant network center is planned in the future to protect against catastrophic events.

Wireless Data

☑ Flexible and dynamic system administration (includes administration of on-scene wireless data networks).	Each agency participating in the CapWIN system administers their own users and functionality. In addition, control of incident creation/modification and communication method (IM, chat, email) is available to all users.

Information Systems

☑ Ability to effectively and efficiently exchange data between agencies/jurisdictions, e.g., by employing common data representation structures and exchange formats and protocols.	CapWIN employs TCP/IP for all communications and XML for all internal data transfers. We are attempting to meet all applicable standards for all external interfaces (Global, 1512, etc.)

Program/Organization:	**CapWIN**

Information Systems

☑ Ability to rapidly access subject information at critical decision points from both field and base locations, including but not limited to information regarding identification (photos, fingerprints, etc.) and activity (criminal history, wants/warrants, reporting/contact history, etc.).	Query access is conducted through VCIN (Virginia), MILES (Maryland), and WALES (D.C.). The capabilities of these systems (none are NCIC2000 compliant) is the limiting factor.

Information Systems

☑ Ability to enter information once, then share and reuse that information among all entities that require it.	CapWIN supports "broadcast" communications though IM/chat/email functionality.

Information Systems

☑ Ability to query/access multiple data sources using one request that is routed to multiple entities simultaneously.	Templar Corporation's Informant product is used to "spawn" transactions to multiple entities and data sources simultaneously. Further, this data is then "fused" and presented intelligently (summary data first, lack of redundant information) to the originating user.

Information Systems

☑ Capability of standardized security, including functions and features that can be used to satisfy reasonable security requirements of any entity within a broader security framework.	All security efforts are geared to the lowest (or highest depending on your perspective) common denominator. Therefore, the system has been designed in such a way as to allow flexibility in security features/methods i.e., encryption methods, authentication/authorization methods, etc. Currently, IBM's Wireless Everyplace Connection Manager handles these functions for the client-side and Cisco and Nortel routers and firewalls handle back-end security and VPN.

Information Systems

☑ Capability of field photo scanning and image file distribution.	Image file distribution is possible though email and instant messaging.

Information Systems

☑ Ability to have near-real-time distribution of text messages to multiple organizations responding to a large event.	Using email and instant messaging and coordinated through the "global directory".

Information Systems

☑ Ability to access information related to hazardous materials, water sources, floor and building plans, utility maps, weather forecasts, topographic terrain, and other background data that may influence how public safety practitioners approach or conduct operations at an incident.	Access to HAZMAT databases/datasources is currently being added to the system.

Information Systems

☑ Ability to access current resource data (including personnel, equipment, materials, etc.) of multiple agencies/jurisdictions responding to a multi-agency/jurisdictional event by authorized users in the respective agencies/jurisdictions.	This is currently only possible through IM and email.

Program/Organization:	**CDC**
Full Name:	Center for Disease Control
Agencies:	HHS
Partnering Agencies / Orgs.:	HHS, CDC
Web Page:	http://www.cdc.gov/aboutcdc.htm
Contact Name:	Melissa Chapman
	Deputy Secretary and Chief, OIRM
Contact Phone:	202-690-6162
Contact Email:	melissa.chapman@hhs.gov

Current Products:	1. Web-based contact information for various threats, agents, and diseases 2. Guidance regarding the public health information technology functions and specifications (see: 'Guidance for Fiscal Year 2002 Supplemental Funds for Public Health Preparedness and Response for Bioterrorism')
Planned Products:	With the 'Doc Alert' system, the Department of Health and Human Services (HHS) plans urgent broadcasts to deployed wireless handheld PDAs that will alert physicians about possible outbreaks of Category A diseases including anthrax, botulism, plague, smallpox, tularemia, and viral hemorrhagic fevers, as well as other types of germ warfare threatening homeland security and public health. Clinicians will be directed to Web sites for additional information. The project will harness technology to allow communication with and among many of the doctors, nurses, and other clinicians who will be called on to diagnose and treat patients quickly in the event of a bioterrorist attack. The Doc Alert system, which is being tested for the next 3 months was developed by [a private firm]. [Telecom Reports 3/25/03]
Additional Information:	Strategic National Stockpile Program (formerly National Pharmaceutical Stockpile) Office of Terrorism Preparedness and Response 1600 Clifton Road, MS D-08 Atlanta, GA 30333 www.bt.cdc.gov 888/246-2675 and 404/639-3311 or 0385 cdcresponse@ashastd.org BTech@cdc.gov HHS : www.hhs.gov/orim/contacts/services.html Dep.Sec & Chief of OIRM = Melissa Chapman 202/690-6162 Telecom = Gary Wall 202/619-0631
Program Goals:	1. To promote health and quality of life by preventing and controlling disease, injury, and disability 2. Timely and high quality data and information for achieving the public health mission

Sectors Addressed:	☐ ***Law Enforcement***	☐ ***Corrections***	☐ ***EMS***	☐ ***Military***
	☐ ***Courts***	☐ ***Probat./Parole***	☑ ***Emerg. Manag.***	☐ ***Other***
	☐ ***Public Defender***	☐ ***Fire Protection***	☐ ***Transportation***	
	☐ ***Prosecution***	☐ ***Public Works***	☐ ***Utlities***	

Program/Organization:	**CJIS**
Full Name:	Criminal Justice Information Services (Division)
Agencies:	DoJ's FBI
Partnering Agencies / Orgs.:	
Web Page:	http://www.fbi.gov/hq/cjisd/cjis.htm
Contact Name:	Dave Walchak
	Deputy Assistant Director, FBI-CJIS
Contact Phone:	202-324-8910
Contact Email:	dwalchak@leo.gov
Current Products:	1. Integrated Automated Fingerprint Identification System (IAFIS) 2. Uniform Crime Reporting (UCR) 3. National Crime Information Center (NCIC) 4. National Incident-Based Reporting System (NIBRS) 5. National Instant Criminal Background Check System (NCIS)
Planned Products:	
Additional Information:	Tom Hopper 202/324-3506 thopper@leo.gov
Program Goals:	Reduce terrorist and criminal activities by maximizing the ability to provide timely and relevant criminal justice information to the FBI and to qualified law enforcement . . . concerning individuals, stolen property, criminal organizations and activities, and other law enforcement related data.

Sectors Addressed:	☑ ***Law Enforcement***	☑ ***Corrections***	☐ ***EMS***	☑ ***Military***
	☑ ***Courts***	☑ ***Probat./Parole***	☑ ***Emerg. Manag.***	☐ ***Other***
	☑ ***Public Defender***	☐ ***Fire Protection***	☐ ***Transportation***	
	☑ ***Prosecution***	☐ ***Public Works***	☐ ***Utlities***	

Functional Capabilities:

Information Systems

☑ Ability to effectively and efficiently exchange data between agencies/jurisdictions, e.g., by employing common data representation structures and exchange formats and protocols.	The CJIS WAN provides connectivity between state agencies. Messages are formatted in accordance with the ANSI/NIST standard for the exchange of fingerprint information and transmitted in a SMTP/MIME envelope.

Program/Organization:	**CJIS**

Information Systems

☑ Ability to rapidly access subject information at critical decision points from both field and base locations, including but not limited to information regarding identification (photos, fingerprints, etc.) and activity (criminal history, wants/warrants, reporting/contact history, etc.).	NCIC has wide availability.

Information Systems

☑ Ability to query/access multiple data sources using one request that is routed to multiple entities simultaneously.	Currently built into the NICS program.

Information Systems

☑ Capability of standardized security, including functions and features that can be used to satisfy reasonable security requirements of any entity within a broader security framework.	All CJIS systems are covered by the CJIS Security Policy developed and approved by the APB.

Information Systems

☑ Ability to exchange information with Computer-Aided Dispatch (CAD) systems.	Many states draw on CJIS services for their CAD systems.

Information Systems

☑ Capability of field photo scanning and image file distribution.	Distributed capture and dissemination of fingerprint images.

Information Systems

☑ Ability to have near-real-time distribution of text messages to multiple organizations responding to a large event.	LEO and NLETS have an alert notification program.

Information Systems

☑ Ability to automatically link disposition data with charge data on subject RAP sheet/CCH information.	We have programs in this area to support NICS and enhance our CCH.

Program/Organization:	**Coast Guard Rescue 21**
Full Name:	Coast Guard National Distress & Response System Modernization Program Phase II (NDRSMP)
Agencies:	DHS, United States Coast Guard
Partnering Agencies / Orgs.:	Coast Guard facilities (e.g., Activities, Groups, Sections, MSOs, Stations, cutters, boats, selected vehicles, and detached personnel), the Coast Guard's customers (e.g., recreational and commercial mariners); other Federal agencies (including the other military services), and state, and local agencies.
Web Page:	http://www.uscg.mil/hq/g-a/ndrsmp/
Contact Name:	Lt. J.G. Sam Edwards
	Public Relations Officer
Contact Phone:	202-267-0902
Contact Email:	sedwards@comdt.uscg.mil
Current Products:	Rescue 21 is currently under development and will be the primary maritime '911' system for U.S. coastal waters and navigable rivers and lakes. The modernized system will interoperate with federal agencies (such as FEMA, DOD, FBI, Secret Service, DEA), and state and local government agencies (such as police forces and emergency service agencies) to support emergencies or natural disasters. The system will use the Project 25-standard VHF radios, and precise direction finding equipment.
Planned Products:	
Additional Information:	Lt. Dan Connolly 202-267-1587 Dconnolly@comdt.uscg.mil 202-267-2229 =HQ Information
Program Goals:	Modernize and upgrade the National Distress and Response System, in order to: Monitor the international VHF-FM distress frequencies of Channel 16 and Channel 70 DSC; Coordinate search and rescue response operations; Communicate with commercial and recreational vessels; Provide command and control (C2) for Coast Guard units (Active, Auxiliary, and Reserve) performing Maritime Safety, Maritime Law Enforcement, National Security, and Marine Environmental Protection missions.

Sectors Addressed:	☑ ***Law Enforcement***	☐ ***Corrections***	☑ ***EMS***	☑ ***Military***
	☐ ***Courts***	☐ ***Probat./Parole***	☑ ***Emerg. Manag.***	☐ ***Other***
	☐ ***Public Defender***	☐ ***Fire Protection***	☑ ***Transportation***	
	☐ ***Prosecution***	☐ ***Public Works***	☐ ***Utlities***	

Functional Capabilities:

Wireless Voice

☑ Ability to initiate wireless voice communications by requiring the user to only enter (on his/her radio) a user identification which authenticates and validates the user, registers and sets talk groups/capabilities for	Rescue 21 provides each regional Group Communication Center (GCC) and mobile unit with Digital Selective Calling (DSC) which provides the capability for automated distress alerting. In addition, Rescue 21 is providing the capability to set up talk groups, as needed, to meet operational requirements.

the user, and completes all radio network administration for the user's voice communications with other members of the user's agency/jurisdiction and with other agencies/jurisdictions, as authorized.	
Wireless Voice	
☑ Ability for users to transparently communicate, as authorized, with other members of the agency/jurisdiction on a unit-to-group (one-to-many) basis and a unit-to-unit (one-to-one) basis.	Rescue 21 will provide unit-to-group (broadcast method) and unit-to-unit (talk group) communications capability.
Wireless Voice	
☑ Ability to communicate an emergency voice message and/or signal which has priority over other voice communications.	Digital Selective Calling (DSC) automatically switches to a voice channel once the initial distress message has been received and acknowledged.
Wireless Voice	
☑ Ability to have secure voice communications.	The new Rescue 21 system will provide 'protected' communications capability (i.e., DES, DES-OFB, AES) at each remote fixed facility within each of the Coast Guard's 46 regions.
Wireless Voice	
☑ Ability for users to transparently communicate, as authorized, among multiple agencies/jurisdictions some of which may use different technologies, infrastructures and/or frequency bands.	Rescue 21 will provide the capability to communicate in the 162-174 MHz and 406-420 MHz bands. In addition, Rescue 21 will provide console-to-console patching capability to link diverse communications systems.
Wireless Voice	
☑ Ability to remotely access a user's agency/jurisdiction voice communications infrastructure when the user roams outside the radio coverage area of the user's agency/jurisdiction wireless infrastructure.	Rescue 21 provides the capability for mobile units to communicate with their home-base when operating outside of their normal radio coverage area through other regional remote fixed facilities via the Coast Guard Data Network.
Wireless Voice	
☑ Ability to effectively initiate and sustain flexible and dynamic system administration (includes administration of talk groups, emergency alerts, networks, and channels for mutual aid).	Rescue 21 provides this capability to each of its 46 regional Group Communication Centers (GCCs).
Wireless Voice	
☑ Ability to sustain highly reliable system performance across interconnected systems (including tolerance to individual system failures, redundant coverage from adjacent sites, resistance to impact of catastrophic events, etc).	Rescue 21 provides guaranteed minimum 99.5% system reliability.
Wireless Voice	
☑ Ability to remotely (over-the-air) reprogram a user's radios and/or modify a user's encryption keys and/or modify a radio's waveforms.	Rescue 21 provides over-the-air reprogramming and over-the-air-rekeying (OTAR) capability for each of its 46 regional Group Communication Centers (GCC).

Wireless Voice

☑ Ability to provide state-wide (county-wide) signal coverage to vehicular/mobile radios on highways and at street level for state (county) agencies, to provide city-wide signal coverage to portable/handheld radios on the street and within buildings for city agencies, and to provide direct communications between user radios when there is no wireless infrastructure to support communications (such in some rural areas, underground parking garages, and inside some buildings).	Rescue 21 is a maritime system and will provide communication coverage out to 20 nm from the territorial sea baseline, the Intracoastal Waterway, navigable harbors, bays, rivers and lakes. Specific coverage areas are defined in the Rescue 21 performance specification.

Wireless Data

☑ Ability to initiate wireless data communications by requiring the user to only enter (on his/her data terminal/radio) a user identification which authenticates and validates the user, registers and sets data resource capabilities for the user, and completes all radio network administration for the user's data communications with other members of the user's agency/jurisdiction and with other agencies/jurisdictions, as authorized.	Digital Selective Calling (DSC) provides this capability.

Wireless Data

☑ Ability of users to quickly and transparently establish on-scene wireless data networks that function among data terminals located in on-scene vehicles and among data terminal carried by users into buildings, etc.	Rescue 21 provides the capability to rapidly transfer data between Coast Guard mobile and shore units. This will greatly enhance the Coast Guard's capability to prosecute search and rescue (SAR) and law enforcement cases, and to track the location and movement of underway Coast Guard assets

Wireless Data

☑ Ability of on-scene personnel to transparently exchange, as authorized, text, image, and/or video data with other on-site personnel, dispatchers, data resources, etc.	Rescue 21 will provide VHF and UHF data exchange capability, including text messaging. The data exchange capability can also be used for automatic chart updating, transmission of search planning data, asset tracking, and much more.

Wireless Data

☑ Ability to protect the privacy of particular information according to applicable laws and statutes so that it can be accessed only by authorized personnel and data terminals.	The new Rescue 21 system will provide 'protected' communications capability (i.e., DES, DES-OFB, AES). Access to sensitive information is controlled at each terminal location.

Wireless Data

☑ Ability to ensure secure exchange of information.	The new Rescue 21 system will provide 'protected' communications capability (i.e., DES, DES-OFB, AES).

Wireless Data

☑ Ability of transparent on-scene system access to multiple information systems regardless of differing data base system architectures and data formats.	Rescue 21 can provide on-scene access to multiple information systems through a gateway located at the Group Communication Center.

Wireless Data

☑ Ability to remotely access a user's agency/jurisdiction data communications infrastructure when the user roams outside the radio coverage area of the user's agency/jurisdiction infrastructure.

Rescue 21 provides the capability for mobile units to access the Coast Guard communications infrastructure when operating outside of their normal operating area through other regional remote fixed facilities and through the Coast Guard Data Network.

Wireless Data

☑ Reliable system operational performance (including fault tolerant to individual system failures, redundant coverage from adjacent sites, full service during routine maintenance, and resistant to impact of catastrophic events).

The Rescue 21 system has a guaranteed operational availability of 99. 5%, which is based on a number of factors, including redundant coverage from adjacent sites, full service during routine maintenance, and resistant to impact of catastrophic events. The Rescue 21 system also includes recovery from catastrophic failure due to disaster to 70% system operation within 24 hours and full operation within 7 days.

Wireless Data

☑ Flexible and dynamic system administration (includes administration of on-scene wireless data networks).

Rescue 21 system administration can be accomplished from any regional communication center via the Coast Guard Data Network.

Information Systems

☑ Ability to enter information once, then share and reuse that information among all entities that require it.

The Coast Guard has this capability through its backbone data network.

Information Systems

☑ Capability of standardized security, including functions and features that can be used to satisfy reasonable security requirements of any entity within a broader security framework.

The new Rescue 21 system will provide "protected" communications capability (i.e., DES, DES-OFB, AES). Access to sensitive information is controlled at each terminal location.

Information Systems

☑ Ability to access information related to hazardous materials, water sources, floor and building plans, utility maps, weather forecasts, topographic terrain, and other background data that may influence how public safety practitioners approach or conduct operations at an incident.

Mission essential applications provide the Coast Guard access to information related to law enforcement, search and rescue, marine safety, aids to navigation, and hazardous materials. Weather forecasts are distributed, via the Coast Guard Data Network and marine information broadcasts, to Coast Guard units and the maritime public.

Program/Organization:	**ComCARE Alliance**
Full Name:	Communications for Coordinated Assistance and Response to Emergencies Alliance
Agencies:	
Partnering Agencies / Orgs.:	More than 90 organizations representing EMS, public safety, emergency management, the wireless industry, automobile and technology companies, telematics suppliers, and citizen groups
Web Page:	http://www.comcare.org/about/overview.html
Contact Name:	David Aylward
	Director
Contact Phone:	202-429-0574
Contact Email:	daylward@comcare.org
Current Products:	o Outreach program o Technology trials o E-Safety Network Initiative o An integrated set of public policy suggestions to upgrade our nation's emergency response communications capabilities
Planned Products:	1. E-Safety Network is an integrated, interoperable, open, Web services architecture for emergency response and emergency management. Field trials supporting all hazards. Development of interoperability tools such a Vehicular Emergency Data Set in XML. 2. GIS-based emergency provider access directory (EPAD) -- A coordinated, comprehensive electronic directory of local agencies, including telephone numbers, Internet addresses, street addresses (and other relevant contact information), emergency Federal, state, and local agencies data type requests. EPAD is a shared, non-profit resource.
Additional Information:	Additional contacts: Art Botterell abotterell@comcare.org
Program Goals:	o to enhance the nation's emergency response systems o to break down institutional barriers to interoperability o to coordinate emergency response databases o to promote interoperability of communications facilities

Sectors Addressed:				
☑	***Law Enforcement***	☐ ***Corrections***	☑ ***EMS***	☐ ***Military***
☐	***Courts***	☐ ***Probat./Parole***	☑ ***Emerg. Manag.***	☐ ***Other***
☐	***Public Defender***	☑ ***Fire Protection***	☑ ***Transportation***	
☐	***Prosecution***	☑ ***Public Works***	☑ ***Utlities***	

Functional Capabilities:

Wireless Voice

☑ Ability for users to transparently communicate, as authorized, with other	Using standards-based data networks and a geospatial directory service to permit instant notifications to agencies based on geographic responsibility /

members of the agency/jurisdiction on a unit-to-group (one-to-many) basis and a unit-to-unit (one-to-one) basis.	interest and other criteria.
Wireless Voice	
☑ Ability for users to transparently communicate, as authorized, among multiple agencies/jurisdictions some of which may use different technologies, infrastructures and/or frequency bands.	Using standards-based data networks and a geospatial directory service to permit instant notifications to agencies based on geographic responsibility / interest and other criteria.
Wireless Voice	
☑ Ability to sustain highly reliable system performance across interconnected systems (including tolerance to individual system failures, redundant coverage from adjacent sites, resistance to impact of catastrophic events, etc).	Using Internet protocols and Web services architecture (including security architecture) for reliable, scaleable, and interoperable voice and data communications.
Wireless Data	
☑ Ability of on-scene personnel to transparently exchange, as authorized, text, image, and/or video data with other on-site personnel, dispatchers, data resources, etc.	Utilizing various public safety and commercial wireless connections to extend the "e-safety network" to individual mobile units.
Wireless Data	
☑ Ability to protect the privacy of particular information according to applicable laws and statutes so that it can be accessed only by authorized personnel and data terminals.	Using public-key infrastructure to implement authentication, non-repudiation, and confidentiality requirements.
Wireless Data	
☑ Ability to ensure secure exchange of information.	Using public-key infrastructure to implement authentication, non-repudiation, and confidentiality requirements.
Wireless Data	
☑ Capability of high speed data transfer to allow fast exchange of text, image, and streaming video information.	Dependent on wireless technologies of participating agencies.
Information Systems	
☑ Ability to effectively and efficiently exchange data between agencies/jurisdictions, e.g., by employing common data representation structures and exchange formats and protocols.	Developing and promoting standards-based message formats such as the XML-based Common Alerting Protocol and hazard-specific formats within a flexible open-standards-based network-centric interoperability architecture.
Information Systems	
☑ Ability to enter information once, then share and reuse that information among all entities that require it.	Using a network-centric messaging architecture to leverage single inputs across all systems that require it.
Information Systems	
☑ Capability of standardized security, including functions and features that can be used to satisfy reasonable security requirements of any entity within a broader security framework.	Utilizing standards-based PKI functions (including WS-Encryption, WS-Signature, and SAML).

Program/Organization: **ComCARE Alliance**

Information Systems

☑ Ability to exchange information with Computer-Aided Dispatch (CAD) systems.

Providing standard interfaces and data unit for system-to-system exchange.

Information Systems

☑ Capability of field photo scanning and image file distribution.

Messaging standards provide for images and other binary objects.

Information Systems

☑ Ability to have near-real-time distribution of text messages to multiple organizations responding to a large event.

Using standards-based data networks and a geospatial directory service to permit instant notifications to agencies based on geographic responsibility / interest and other criteria.

Information Systems

☑ Ability to access information related to hazardous materials, water sources, floor and building plans, utility maps, weather forecasts, topographic terrain, and other background data that may influence how public safety practitioners approach or conduct operations at an incident.

Providing shared situational awareness and geospatial information from multiple data sources on a map interface, or to any other IP address(es) the subscriber designates. Encouraging the development and sharing of such on-line resources due to standards basis of the E-Safety Network, and the national market it would create for vendors.

Information Systems

☑ Ability to access medical/treatment records (both those required to ensure proper treatment of incident victims and/or prisoners and those records obtained under warrant).

Yes. Some of our members are prepared to do exactly this. We see this in the same way that the prior question suggested that there are multiple data sources that may be related to an incident.

Information Systems

☑ Ability to access current resource data (including personnel, equipment, materials, etc.) of multiple agencies/jurisdictions responding to a multi-agency/jurisdictional event by authorized users in the respective agencies/jurisdictions.

The E-Safety Network is designed to enable exactly this. It now shows hospital availability, but any resource information can be shared.

Program/Organization:	**COPS**
Full Name:	Community Oriented Policing Services
Agencies:	DOJ
Partnering Agencies / Orgs.:	Tribal, state, local law enforcement agencies
Web Page:	http://www.cops.usdoj.gov/
Contact Name:	Nancy Leach, Mike Dame
Contact Phone:	202-514-8252 202-305-7451
Contact Email:	nancy.leach@usdoj.gov Michael.Dame2@usdoj.gov
Current Products:	1. 12,950 jurisdictions have been helped through 27 different grants programs for hiring and training community policing professionals, 2. Funds for 116,573 community policing professionals across the country
Planned Products:	Interoperable Communications Technology Program
Additional Information:	Additional phone numbers: 1-800-421-6770 202-307-1480
Program Goals:	1. To craft grant programs responsive to the needs of state, local, and tribal law enforcement from the funding available in the 1994 bill 2. To advance community policing (focusing on crime prevention) in jurisdictions of all sizes across the United States 3. To provide grants to tribal, state, and local law enforcement for law-enforcement training.

Sectors Addressed:				
☑ ***Law Enforcement***	☐ ***Corrections***	☑ ***EMS***	☐ ***Military***
☐ ***Courts***	☐ ***Probat./Parole***	☐ ***Emerg. Manag.***	☐ ***Other***
☐ ***Public Defender***	☑ ***Fire Protection***	☐ ***Transportation***	
☐ ***Prosecution***	☐ ***Public Works***	☐ ***Utlities***	

Functional Capabilities:

Wireless Voice

☑ Ability to initiate wireless voice communications by requiring the user to only enter (on his/her radio) a user identification which authenticates and validates the user, registers and sets talk groups/capabilities for the user, and completes all radio network administration for the user's voice communications with other members of the user's agency/jurisdiction and with other agencies/jurisdictions, as authorized.

Support the development of standards by validating proposed specifications through laboratory testing. Support the interoperability testing of standardized products by acquiring test suites of Project 25 radio equipment.

Program/Organization:	**COPS**

Wireless Voice

☑ Ability for users to transparently communicate, as authorized, with other members of the agency/jurisdiction on a unit-to-group (one-to-many) basis and a unit-to-unit (one-to-one) basis.	Support the development of standards by validating proposed specifications through laboratory testing. Support the interoperability testing of standardized products by acquiring test suites of Project 25 radio equipment.

Wireless Voice

☑ Ability of the agency/jurisdiction to administer the priority for voice communications of particular users and particular applications (such as task force operations, incidents, etc.).	In conjunction with Project MESA, standardization related to quality of service (QOS) and priority access parameters.

Wireless Voice

☑ Ability for users to transparently communicate, as authorized, among multiple agencies/jurisdictions some of which may use different technologies, infrastructures and/or frequency bands.	Support the development of standards by validating proposed specifications through laboratory testing. Support the testing of interoperability products by acquiring test suites of equipment.

Wireless Voice

☑ Ability to remotely access a user's agency/jurisdiction voice communications infrastructure when the user roams outside the radio coverage area of the user's agency/jurisdiction wireless infrastructure.	Support the development of standards by validating proposed specifications through laboratory testing. Support the testing of interoperability products by acquiring test suites of equipment.

Wireless Voice

☑ Ability to sustain highly reliable system performance across interconnected systems (including tolerance to individual system failures, redundant coverage from adjacent sites, resistance to impact of catastrophic events, etc).	Wireless research and standardization of performance in adverse environments in conjunction with Project MESA, etc.

Wireless Voice

☑ Ability to provide state-wide (county-wide) signal coverage to vehicular/mobile radios on highways and at street level for state (county) agencies, to provide city-wide signal coverage to portable/handheld radios on the street and within buildings for city agencies, and to provide direct communications between user radios when there is no wireless infrastructure to support communications (such in some rural areas, underground parking garages, and inside some buildings).	Research, analysis, and development efforts related to the propagation of Wireless Communications Signals through Building Structures, Urban Environments, and debris, considering existing and emerging wireless technologies. In addition, evaluation of alternatives for communicating in the same environments, e.g., using fixed and mobile intra-building repeaters.

Wireless Data

☑ Ability to initiate wireless data communications by requiring the user to only enter (on his/her data terminal/radio) a user identification which authenticates and validates the user, registers and sets data resource capabilities for the user, and completes all radio network administration for the user's data communications with other members of the user's agency/jurisdiction and with other agencies/jurisdictions, as authorized.

Support the development of standards by validating proposed specifications through laboratory testing. Support the interoperability testing of standardized products by acquiring test suites of Project 25 radio equipment.

Wireless Data

☑ Ability of users to quickly and transparently establish on-scene wireless data networks that function among data terminals located in on-scene vehicles and among data terminal carried by users into buildings, etc.

Standardization of wireless approaches satisfying public safety requirements by working within such standards development bodies as Internet Engineering Task Force (IETF) and the Institute of Electrical and Electronics Engineers Standards Committee 802 (IEEE 802).

Wireless Data

☑ Ability of on-scene personnel to transparently exchange, as authorized, text, image, and/or video data with other on-site personnel, dispatchers, data resources, etc.

Standardization of wireless approaches after defining, in conjunction with public safety practitioners and Project MESA, functional/operational requirements in urban settings for voice, data, image, and video.

Wireless Data

☑ Ability to protect the privacy of particular information according to applicable laws and statutes so that it can be accessed only by authorized personnel and data terminals.

Standardization in conjunction with AGILE Program, Project 25/TIA TR 8, Software Defined Radio Forum, NPSTC SDR Working Group, SAFECOM, etc.

Wireless Data

☑ Capability of high speed data transfer to allow fast exchange of text, image, and streaming video information.

In conjunction with Project MESA and IAB, standardization of approaches for transferring critical building information (e.g., fire alarms, temperature, heat generation rates, etc.) to fixed and mobile sites.

Wireless Data

☑ Ability of transparent on-scene system access to multiple information systems regardless of differing data base system architectures and data formats.

In conjunction with Project MESA, IAB, and GLOBAL, standardization of procedures for acquiring and transferring building data.

Information Systems

☑ Ability to effectively and efficiently exchange data between agencies/jurisdictions, e.g., by employing common data representation structures and exchange formats and protocols.

Laboratory support to Information Technology Interoperability Standardization in conjunction with the Global Justice Information Sharing Initiative ('Global') Advisory Committee, and its Infrastructure/Standards Working Group.

Information Systems

☑ Ability to rapidly access subject information at critical decision points from both field and base locations, including but not limited to information regarding identification (photos, fingerprints, etc.) and activity (criminal history, wants/warrants, reporting/contact history, etc.).

Laboratory support to standardization in conjunction with GLOBAL Standards Committees, Project 25/TIA TR 8, Software Defined Radio Forum, NPSTC SDR Working Group, SAFECOM, etc.

Program/Organization:	**COPS**

Information Systems

☑ Capability of standardized security, including functions and features that can be used to satisfy reasonable security requirements of any entity within a broader security framework.	As a direct complement to the standardization of information sharing approaches occurring through GLOBAL Infrastructure/Standards Working Group, and in conjunction with the Federal CIO Council and XML.gov efforts related with the ebXML Registry, the design and development of an effective and efficient security model.

Information Systems

☑ Ability to have near-real-time distribution of text messages to multiple organizations responding to a large event.	Laboratory support to standardization in conjunction with GLOBAL Standards Committees, Project 25/TIA TR 8, Software Defined Radio Forum, NPSTC SDR Working Group, SAFECOM, and IEEE 1512.

Information Systems

☑ Ability to access information related to hazardous materials, water sources, floor and building plans, utility maps, weather forecasts, topographic terrain, and other background data that may influence how public safety practitioners approach or conduct operations at an incident.	Research and development related to the use of new and emerging wireless transceiver/sensor technologies aimed at providing temporary situational awareness and direct communication links for first responders. Standardization in conjunction with GLOBAL Standards Committees and the InterAgency Board for Equipment Standardization and Interoperability (IAB).

Information Systems

☑ Ability to access information regarding pending investigation/litigation of a particular subject.	Standardization in conjunction with GLOBAL Standards Committees.

Information Systems

☑ Ability to access current resource data (including personnel, equipment, materials, etc.) of multiple agencies/jurisdictions responding to a multi-agency/jurisdictional event by authorized users in the respective agencies/jurisdictions.	Standardization in conjunction with GLOBAL Standards Committees, IAB, IEEE 1512, and Project MESA.

Program/Organization:	**DEA / NDPIX**
Full Name:	Drug Enforcement Administration/National Drug Pointer Index Program
Agencies:	DoJ
Partnering Agencies / Orgs.:	Federal, State, and Local Law Enforcement
Web Page:	http://www.usdoj.gov/dea/
Contact Name:	Mina Hunter
	Acting Chief, NDPIX
Contact Phone:	202-307-3648
Contact Email:	mhunter@leo.gov

Current Products:	1. National Drug Pointer Index, operational since 1997 (that allows state and local LE to determine if other LE organizations were investigating the same drug suspect) 2. Intelligence programs 3. Training programs for drug-trade interdiction 4. Management of a national drug intelligence program in cooperation with Federal, state, local, and foreign officials to collect, analyze, and disseminate strategic and operational drug intelligence information. 5. Coordination and cooperation with Federal, state, and local law enforcement officials (through IDEA--Integrated Drug Enforcement Assistance) to accomplish the following: a. Cooperate on mutual drug enforcement efforts and enhancement of such efforts through exploitation of potential interstate and international investigations beyond local or limited Federal jurisdictions and resources b. Cooperate in programs designed to reduce the availability of illicit abuse-type drugs on the U.S. market through methods such as crop eradication, crop substitution, and training of foreign officials. 6. Programs such as: a. Marijuana eradication b. Mobile Enforcement Teams c. Southwest Border Initiative, etc. DEA is currently working with representatives from 24 Federal, state, and local law enforcement agencies and organizations representing 19 states to develop and implement a National Drug Pointer Index (NDPIX) that will greatly enhance coordination among drug law enforcement entities. By accessing the system's database, participating law enforcement agencies will be able to determine quickly whether a current drug suspect is under active investigation by another participating agency. NDPIX will provide point of contact information only
Planned Products:	
Additional Information:	Judith Bertini, Deputy Assistant Administrator for intelligence 202/307-8748 jbertini@leo.gov
Program Goals:	1. Enhance the personal safety of law enforcement personnel; 2. Promote information sharing among law enforcement agencies; 3. Provide a means for participating agencies to identify common investigative targets; 4. Increase interagency cooperation and foster joint drug investigations.

Program/Organization:	**DEA / NDPIX**			
Sectors Addressed:	☑ *Law Enforcement*	☐ *Corrections*	☐ *EMS*	☐ *Military*
	☐ *Courts*	☐ *Probat./Parole*	☐ *Emerg. Manag.*	☐ *Other*
	☐ *Public Defender*	☐ *Fire Protection*	☐ *Transportation*	
	☐ *Prosecution*	☐ *Public Works*	☐ *Utlities*	

Program/Organization:	**DoT ITS Program**
Full Name:	Department of Transportation - Intelligent Transportation System
Agencies:	U.S. DoT: Federal Highway Administration (FHWA) National Highway Traffic Safety Admin (NHTSA) Federal Transit Administration (FTA) Federal Motor Carrier Safety Admin (FMCSA)
Partnering Agencies / Orgs.:	U.S. Fire Administration (U.S. DHS) Office of Justice Programs (U.S. DoJ)
Web Page:	http://www.its.dot.gov/
Contact Name:	Craig Allred
	Public Safety Coordinator
Contact Phone:	202-366-8034
Contact Email:	craig.allred.@fhwa.dot.gov
Current Products:	Wireless Enhanced 9-1-1: See http://www.itspublicsafety.net/wireless.htm Emergency Medical Services: See http://www.itspublicsafety.net/its_americapublicsafety_ems.htm Fire & Rescue: See http://www.itspublicsafety.net/fire.htm Law Enforcement: See http://www.itspublicsafety.net/law_itsmanagement.htm Articles & Case Studies: See http://www.itspublicsafety.net/articles.htm Standards: See http://www.its-standards.net/Documents/FSP1512_r2.PDF
Planned Products:	1. Documents identifying the benefits of integrated deployments of metro ITS infrastructure.
Additional Information:	Mr. Ken Brooke ken@mitretek.org phone: (202) 488-5719 fax: (202) 554-7309 The ITS Public Safety Program web page: http://www.itspublicsafety.net/ The ITS Standards Program web page: http://www.its-standards.net/
Program Goals:	The ITS Public Safety Program encourages transportation and public safety agencies to better integrate their on-scene incident response, clearance and recovery operations. The Program fosters new partnerships between transportation and public safety agencies to develop more interoperable communications systems and incident management procedures. The ITS Public Safety Program is working to improve emergency services through: o Faster incident detection and notification o Faster emergency response times, and o Real-time wireless communications links among emergency response organizations

Sectors Addressed:	☑ ***Law Enforcement***	☐ ***Corrections***	☑ ***EMS***	☐ ***Military***
	☐ ***Courts***	☐ ***Probat./Parole***	☐ ***Emerg. Manag.***	☑ ***Other***
	☐ ***Public Defender***	☑ ***Fire Protection***	☑ ***Transportation***	***HAZMAT***
	☐ ***Prosecution***	☑ ***Public Works***	☐ ***Utlities***	

Functional Capabilities:

Wireless Voice

☑ Ability to provide state-wide (county-wide) signal coverage to vehicular/mobile radios on highways and at street level for state (county) agencies, to provide city-wide signal coverage to portable/handheld radios on the street and within buildings for city agencies, and to provide direct communications between user radios when there is no wireless infrastructure to support communications (such in some rural areas, underground parking garages, and inside some buildings).	System coverage includes locations within transportation structures (e.g., under bridges, within tunnels).

Wireless Data

☑ Ability to initiate wireless data communications by requiring the user to only enter (on his/her data terminal/radio) a user identification which authenticates and validates the user, registers and sets data resource capabilities for the user, and completes all radio network administration for the user's data communications with other members of the user's agency/jurisdiction and with other agencies/jurisdictions, as authorized.	

Wireless Data

☑ Ability of on-scene personnel to transparently exchange, as authorized, text, image, and/or video data with other on-site personnel, dispatchers, data resources, etc.	

Wireless Data

☑ Capability of high speed data transfer to allow fast exchange of text, image, and streaming video information.	Highway TV camera video, available from some traffic management centers, is compressed NTSC video.

Wireless Data

☑ Ability of transparent on-scene system access to multiple information systems regardless of differing data base system architectures and data formats.	ITS would prefer that there be only one interface between transportation and public safety information systems.

Information Systems

☑ Ability to effectively and efficiently exchange data between agencies/jurisdictions, e.g., by employing common data representation structures and exchange formats and protocols.	IEEE Standard 1512 was specifically designed to address this requirement, in the domain of transportation incidents.

Information Systems

☑ Ability to enter information once, then share and reuse that information among all entities that require it.	This is not a requirement, but an objective. Particularly within and among a multi-agency, or multi-disciplinary response to an incident.

Information Systems

☑ Ability to exchange information with Computer-Aided Dispatch (CAD) systems.

Information Systems

☑ Ability to have near-real-time distribution of text messages to multiple organizations responding to a large event.

Information Systems

☑ Ability to access information related to hazardous materials, water sources, floor and building plans, utility maps, weather forecasts, topographic terrain, and other background data that may influence how public safety practitioners approach or conduct operations at an incident.

Particularly information related to transportation systems, including transit systems, and particularly including traffic congestion and infrastructure condition information.

Program/Organization:	**EPG / CTAC Technology Transfer Program**
Full Name:	Electronic Proving Grounds, Technology Transfer Program for ONDCP/CTAC
Agencies:	U.S. Department of the Army
Partnering Agencies / Orgs.:	U.S. Army Electronic Proving Grounds (Special Program Office) ONDCP / CTAC
Web Page:	www.epgctac.com
Contact Name:	Lt. Col. L.J. Schnider
Contact Phone:	1-877-EPG-CTAC
Contact Email:	ttp@epgctac.com
Current Products:	The Technology Transfer Program has the following available: o ACISS Narcotics & Intelligence Records Management System o Advanced Digital Audio Collection System (ADACS) o Audio Surveillance System o Advanced Vehicle Tracking System (AVTS) o Body Worn - Miniaturized covert audio device o Cellular-Based Surveillance System (CBSS) o Digital Information Gateway (DIG) o Digital Pager Intercept o Drugwipe, Drug Test Kit o Interoperability Communications System (ICS) o Local Intercept Network Collection - On Line Network (LINCOLN) wiretap system o Mini-Buster Contraband Detector o MiniPIX Wireless Video Surveillance o Multimedia Processing System (MPS) o Night Vision Kit o Pen-Link Analysis Software o PicoDAC o R3000 Navigator Telephone Surveillance System o Sentinel Vehicle Tracking System o Suspect Pointer Index Network (SPIN) o Stedi-Eye Observer o Thermal Imager o ThermoVision Scout o VideoDetective Interceptor o VisuaLinks Software o VoiceBox System
Planned Products:	
Additional Information:	EPG Counterdrug Office (toll free) 1-877-374-2822 http://www.nlectc.org/equipment/ctac.html Rafael Anton 520-538-4916

Program/Organization:	**EPG / CTAC Technology Transfer Program**
Program Goals:	1. To develop and implement the National Counterdrug Enforcement Research and Development Strategy, which identifies and defines the scientific and technological needs of Federal, state, and local drug enforcement agencies. 2. The CTAC Technology Transfer program transfers counterdrug systems and devices directly to state and local law enforcement agencies that might otherwise be unable to profit from new equipment due to limited budgets.

Sectors Addressed:				
	☑ *Law Enforcement*	☐ *Corrections*	☐ *EMS*	☐ *Military*
	☐ *Courts*	☐ *Probat./Parole*	☐ *Emerg. Manag.*	☐ *Other*
	☐ *Public Defender*	☐ *Fire Protection*	☐ *Transportation*	
	☐ *Prosecution*	☐ *Public Works*	☐ *Utlities*	

Program/Organization:	**FCC**
Full Name:	Federal Communications Commission/Public Safety & Private Wireless Division
Agencies:	
Partnering Agencies / Orgs.:	
Web Page:	http://wireless.fcc.gov/publicsafety/
Contact Name:	Jeanne Kowalski
	Deputy Chief (Safety), Public Safety & Private Wireless Division
Contact Phone:	202-418-0680
Contact Email:	jkowalsk@fcc.gov
Current Products:	See http://wireless.fcc.gov/publicsafety/
Planned Products:	
Additional Information:	Additional contact: Mr. Greg Intoccia, Special Counsel, Public Safety & Private Wireless Division gintocci@fcc.gov 202-418-1470
Program Goals:	The Federal Communications Commission (FCC) is an independent federal agency, directly responsible to Congress. The FCC's Public Safety & Private Wireless Division is part of the FCC's Wireless Telecommunications Bureau. The FCC is charged with regulating interstate and international communications by radio, television, wire, satellite, and cable, and has as a purpose promoting safety of life and property through the use of wire and radio communications.

Sectors Addressed:				
☑ ***Law Enforcement***	☑ ***Corrections***	☑ ***EMS***	☐ ***Military***
☑ ***Courts***	☑ ***Probat./Parole***	☑ ***Emerg. Manag.***	☑ ***Other***
☐ ***Public Defender***	☑ ***Fire Protection***	☑ ***Transportation***	***Aviation, Maritime and Ham Radio,***
☐ ***Prosecution***	☑ ***Public Works***	☑ ***Utlities***	

Program/Organization:	**Federal CIO Council**
Full Name:	Federal Chief Information Officers Council
Agencies:	Federal Architecture & Infrastructure Committee XML Working Group of CIO Council; XML.gov
Partnering Agencies / Orgs.:	
Web Page:	http://www.cio.gov
Contact Name:	Norman Lorentz
	Director, AIC
Contact Phone:	202-395-0370
Contact Email:	nlorentz@omb.eop.gov
Current Products:	
Planned Products:	
Additional Information:	
Program Goals:	1. To improve practices for the management of information technology. 2. To provide a critical foundation for eGovernment by supporting the development of a government-wide enterprise architecture and infrastructure and by providing models and standards for Federal systems and services. 3. To improve the Federal government's ability to attract and retain a top-notch IT workforce, and to expand effective IT education and training opportunities for the existing Federal workforce.

Sectors Addressed:	☐ ***Law Enforcement***	☐ ***Corrections***	☐ ***EMS***	☐ ***Military***
	☐ ***Courts***	☐ ***Probat./Parole***	☐ ***Emerg. Manag.***	☑ ***Other***
	☐ ***Public Defender***	☐ ***Fire Protection***	☐ ***Transportation***	***All Federal users***
	☐ ***Prosecution***	☐ ***Public Works***	☐ ***Utlities***	

Program/Organization:	**FLEWUG**
Full Name:	Federal Law Enforcement Wireless Users' Group
Agencies:	U.S. Department of Justice U.S. Treasury Department
Partnering Agencies / Orgs.:	More than 30 Federal departments and agencies with public safety missions responsible for law enforcement, urban and wildland fire fighting, search and rescue, and emergency response activities.
Web Page:	
Contact Name:	Jim Downes
	Program Manager
Contact Phone:	202-622-2985
Contact Email:	james.downes@do.treas.gov
Current Products:	o Forum for Federal radio spectrum users to address interoperability.
Planned Products:	
Additional Information:	
Program Goals:	o Develop innovative wireless communications technologies (working with industry on several key issues) to meet the needs of public safety (PS) wireless users o Ensure that priority access is afforded to public safety personnel o Promote the availability of commercial services in less populous areas where PS agencies must operate o Promote nearly instantaneous connectivity for PS personnel during emergencies o Promote security measures and encryption that meet minimum Federal requirements o Plan and coordinate future, shared-use, wireless communications systems and resources o Provide a forum for federal radio spectrum users to address interoperability

Sectors Addressed:	☑ ***Law Enforcement***	☐ ***Corrections***	☐ ***EMS***	☐ ***Military***
	☐ ***Courts***	☐ ***Probat./Parole***	☑ ***Emerg. Manag.***	☑ ***Other***
	☐ ***Public Defender***	☑ ***Fire Protection***	☐ ***Transportation***	***Search and Rescue***
	☐ ***Prosecution***	☐ ***Public Works***	☐ ***Utlities***	

Program/Organization:	**FWUF**
Full Name:	Federal Wireless Users' Forum
Agencies:	DoC, NSA, NCS
Partnering Agencies / Orgs.:	o NTIA o GSA o DoJ o DHS o NIST o PSWN o DOD o FBI
Web Page:	http://www-x.antd.nist.gov/fwuf/object.html
Contact Name:	Jeng Mao (NTIA)
	Co-chair, FWUF
Contact Phone:	202-482-9131
Contact Email:	jmao@ntia.doc.gov
Current Products:	Federal Wireless Policy Committee (FWPC) documents: o Current and Future Functional Requirements for Federal Wireless Services in the United States, Revision December 2001 o Federal User's Wireless Telephone Security Risks
Planned Products:	The Federal Wireless Users' Forum is a clearinghouse for information about wireless telecommunications technologies and policies. To provide that information the Forum will provide: o multi-day workshops with industry participation o outreach work sessions with a focus on a particular user community o development of user application profiles
Additional Information:	Workshops take place twice a year, Spring and Fall, on both coasts.
Program Goals:	o To educate Federal government users about wireless telecommunications o To identify the telecommunication needs of Federal government users o To facilitate information exchange with other user groups, standards organizations, manufacturers, and service providers to ensure that government user needs are met o To support the interoperability of emerging wireless services and equipment through increased participation in the formulation of Federal policy, support of standardization efforts, and other appropriate activities.

Sectors Addressed:				
☐ ***Law Enforcement***	☐ ***Corrections***	☐ ***EMS***	☐ ***Military***
☐ ***Courts***	☐ ***Probat./Parole***	☐ ***Emerg. Manag.***	☑ ***Other***
☐ ***Public Defender***	☐ ***Fire Protection***	☐ ***Transportation***	***All Federal users***
☐ ***Prosecution***	☐ ***Public Works***	☐ ***Utlities***	

Program/Organization:	**GLOBAL**
Full Name:	Global Justice Information Sharing Initiative
Agencies:	DoJ, BJA
Partnering Agencies / Orgs.:	DoJ, NIJ, OST, OJP, BJA U.S. Attorney General International Association of Chiefs of Police INTERPOL FBI / CJIS NASCIO National Center for State Courts National Association for Court Management SEARCH NLETS
Web Page:	http://www.it.ojp.gov/
Contact Name:	Tom Henderson
	Chair, ISWG
Contact Phone:	703-841-0200 x5600
Contact Email:	thenderson@ncsc.dni.us
Current Products:	1. XML Data Dictionary (DD): The Justice Data Dictionary, April 2003 edition, version 3.0, contains some 2000 standardized data element definitions as well as principles and guidelines for justice and public-safety XML specification development. The document also contains tag name guidelines, element content & enumeration guidelines, and a list of accepted abbreviations and acronyms for use in tag names. Information is also given on the recommended data format, the inclusion policy, the extension policy, and additional requirements. This DD has been released for comment and is posted on the Web at http://www.it.ojp.gov (then click on the "Justice XML Data Model" tab). 2. Lessons Learned in Reconciling Three Justice XML DDs: This June 2002 document delineates principles of XML development used in reconciling three major specifications efforts within the justice and public-safety communities; it provides excellent background for confronting similar issues associated with interoperability and information sharing among local, tribal, state, and Federal entities. 3. JSC (Justice Standards Clearinghouse) for Information Sharing: This repository contains 73 justice and public-safety standards and specifications that promote information sharing. It also contains reviewer comments, help files (for users who are entering standards), and a tailored search engine. More standards are scheduled for inclusion in the Clearinghouse at http://it.ojp.gov/jsr/public/login.jsp
Planned Products:	1. Updates to the XML Data Dictionary 2. Updates and additions to the Justice Standards Clearinghouse
Additional Information:	Additional contact: Gerry Wethington 573/526-7741 wethig@mail.oit.state.mo.us
Program Goals:	1. To promote information sharing among the justice and public-safety communities. 2. To recommend, via the U.S. Attorney General et al., actions and approaches to facilitate effective information sharing and integration.

Program/Organization:	**GLOBAL**			
Sectors Addressed:	☑ *Law Enforcement*	☑ *Corrections*	☐ *EMS*	☐ *Military*
	☑ *Courts*	☑ *Probat./Parole*	☐ *Emerg. Manag.*	☐ *Other*
	☑ *Public Defender*	☐ *Fire Protection*	☐ *Transportation*	
	☑ *Prosecution*	☐ *Public Works*	☐ *Utlities*	

Program/Organization:	**GuardNet XXI**
Full Name:	Guard Net XXI
Agencies:	National Guard Bureau
Partnering Agencies / Orgs.:	National Guard Bureau Civilian Agencies
Web Page:	http://www.sra.com/services/network.html
Contact Name:	Lt. Col. Michael Jones
Contact Phone:	703-607-5815
Contact Email:	michael.jones6@us.army.mil

Current Products:	A high-speed network that is shared, and has dual-use mechanisms that bridge the military and the civilian sectors. In the Anthrax scare following 9-11, the Guard used the network at the request of the CDC to broadcast programs about the deadly substance
Planned Products:	
Additional Information:	Chief of the National Guard Bureau is Lt. General H. Steven Blum additional web site: www.ngb.army.mil additional email: michael.j.jones@aisco.ngb.army.mil
Program Goals:	o to provide network support services 24 x 7 o to provide a shared, dual-use mechanism that bridges the military and the civilian sectors o to offer readiness training o to offer command-and-control capabilities o to offer readiness training and information for civilian first responders in emergencies o to consolidate video and data communications functions to support readiness, mobilization, command and control, and computer emergency response in addition to the various missions assigned to the National Guard (including C4I, distance learning, disaster assistance, incident response, and information operations)

Sectors Addressed:	☐ ***Law Enforcement***	☐ ***Corrections***	☐ ***EMS***	☑ ***Military***
	☐ ***Courts***	☐ ***Probat./Parole***	☐ ***Emerg. Manag.***	☐ ***Other***
	☐ ***Public Defender***	☐ ***Fire Protection***	☐ ***Transportation***	
	☐ ***Prosecution***	☐ ***Public Works***	☐ ***Utlities***	

Program/Organization:	**HSSP**
Full Name:	Homeland Security Standards Panel
Agencies:	American National Standards Institute (ANSI)
Partnering Agencies / Orgs.:	Panel membership is open to all materially affected U.S.-domiciled parties. At a minimum, the members of the HSSP will reflect each of the 14 critical sectors of Homeland Security as identified by the Federal Government: Agriculture, Government, Banking and Finance, Information and Telecommunications, Chemical Industry and Hazardous Materials, National Monuments and Icons, Defense Industrial Base, Postal and Shipping, Emergency Services, Public Health, Energy Transportation, Food, Water
Web Page:	http://www.ansi.org
Contact Name:	Mary Saunders and Dan Bart Co-Chairs, HSSP
Contact Phone:	301-975-2396 & 703-907-7703
Contact Email:	mary.saunders@nist.gov dbart@tiaonline.org
Current Products:	Web site www.nssn.org lists ~50,000 standards (International & National standards), ANSI standards, and mil specs, all with cross references to the 'Federal Register'.
Planned Products:	1. A web site with a portal that lists who is working on what standards. 2. ANSI-sponsored conference on Homeland Security Issues (Sept. 2003) 3. Database (catalog) of consensus standards responsive to Homeland Security needs 4. Assistance in development of Homeland Security and emergency preparedness standards.
Additional Information:	David Karmol, VP Public Policy & Gov. 202/331-3610 dkarmol@ansi.org Matthew Deane, HSSP Secretary 212/642-4992 mdeane@ansi.org Steve Oksala 1-800-542-5040 is Chair of ANSI's National Policy Committee
Program Goals:	1. To catalog (on the Web), promote, accelerate, and coordinate the timely development of consensus standards within the national and international voluntary standards system intended to meet identified Homeland Security needs, and to communicate the existence of such standards appropriately to governmental units and the private sector. 2. To facilitate the timely development and adoption of standards responsive to the National Strategy for Homeland Security and other identified Homeland Security needs. 3. Where standards do not exist, obtain agreement from a standards developer to initiate development of the standard in a timely manner. 4. To promote collaborative efforts.

Sectors Addressed:				
☑ ***Law Enforcement***	☐ ***Corrections***	☑ ***EMS***	☑ ***Military***
☐ ***Courts***	☐ ***Probat./Parole***	☑ ***Emerg. Manag.***	☑ ***Other***
☐ ***Public Defender***	☑ ***Fire Protection***	☑ ***Transportation***	
☐ ***Prosecution***	☑ ***Public Works***	☑ ***Utlities***	

Program/Organization:	**IAB**
Full Name:	Interagency Board for Equipment Standardization and Interoperability
Agencies:	DoJ
Partnering Agencies / Orgs.:	DoJ, DHS, NIST/OLES, DoD, state and local first-responder agencies
Web Page:	http://www.iab.gov/IAB.asp
Contact Name:	Alan D. Vickery
	Chair of IAB
Contact Phone:	206-386-1895
Contact Email:	alan.vickery@ci.seattle.wa.us
Current Products:	A Standardized Equipment List (SEL) for the equipment (including telecommunications gear) required to prepare for, respond to, mitigate, and recover from a CBRNE incident. http://www.iab.gov/SEL/sel2001.htm
Planned Products:	1. Single-source compendium for first responders. This compendium describes available equipment for responding to WMD events 2. A published set of first-responder equipment guides 3. Respirator standards (with National Institute of Occupational Safety and Health (NIOSH)) 4. Identifying CBRNE incident response equipment requirements 5. Assisting in the development and implementation of performance criteria, standards, and test protocols for SLE-listed CBRNE incident response equipment
Additional Information:	Robert Ingram, 212-860-9230 BobLINY@aol.com
Program Goals:	To establish and coordinate local, state, and Federal standardization, interoperability, and responder safety to prepare for, respond to, mitigate, and recover from any incident by identifying requirements for chemical, biological, radiological, nuclear, or explosives (CBRNE) incident response equipment.

Sectors Addressed:			
☑ ***Law Enforcement***	☐ ***Corrections***	☑ ***EMS***	☑ ***Military***
☐ ***Courts***	☐ ***Probat./Parole***	☑ ***Emerg. Manag.***	☐ ***Other***
☐ ***Public Defender***	☑ ***Fire Protection***	☐ ***Transportation***	
☐ ***Prosecution***	☐ ***Public Works***	☐ ***Utlities***	

Program/Organization:	**IACP**
Full Name:	International Association of Chiefs of Police
Agencies:	APCO, and others
Partnering Agencies / Orgs.:	1. Law Enforcement 2. First Responders
Web Page:	http://www.theiacp.org/
Contact Name:	Harlin McEwen
	Chairman, Communications and Technology Committee
Contact Phone:	607-257-1522
Contact Email:	ChiefHRM@leo.gov
Current Products:	
Planned Products:	
Additional Information:	Matt Snyder 800-843-4227 x 315 snyderm@theiacp.org Jennifer Hicks 800-843-4227 x275 hicksj@theiacp.org
Program Goals:	1. Improved law enforcement 2. Training for improved law enforcement

Sectors Addressed:

☑ *Law Enforcement*	☐ *Corrections*	☐ *EMS*	☐ *Military*
☐ *Courts*	☐ *Probat./Parole*	☐ *Emerg. Manag.*	☐ *Other*
☐ *Public Defender*	☐ *Fire Protection*	☐ *Transportation*	
☐ *Prosecution*	☐ *Public Works*	☐ *Utlities*	

Program/Organization:	**IAFC**
Full Name:	International Association of Fire Chiefs
Agencies:	
Partnering Agencies / Orgs.:	APCO International, Inc.
Web Page:	http://www.iafc.org
Contact Name:	Alan Caldwell
	Director of Government Relations
Contact Phone:	703-273-9815 x309
Contact Email:	acaldwell@iafc.org
Current Products:	
Planned Products:	
Additional Information:	
Program Goals:	The IAFC is a professional association of fire and emergency service leaders whose purpose is professional development, information sharing, and representation at the Federal government.

Sectors Addressed:

☐ *Law Enforcement*	☐ *Corrections*	☑ *EMS*	☐ *Military*
☐ *Courts*	☐ *Probat./Parole*	☐ *Emerg. Manag.*	☐ *Other*
☐ *Public Defender*	☑ *Fire Protection*	☐ *Transportation*	
☐ *Prosecution*	☐ *Public Works*	☐ *Utlities*	

Program/Organization:	**IEEE 1512**
Full Name:	Institute of Electrical and Electronics Engineers (IEEE), Committee 1512
Agencies:	National Association and Standards Development Organization (SDO)
Partnering Agencies / Orgs.:	1. IT and wireless experts 2. Representatives from academia, government, and industry (in the standards-development process)
Web Page:	http://www.ieee.org
Contact Name:	Ann Lorscheider
	Chair, IEEE Incident Management Working Group
Contact Phone:	704-342-6814
Contact Email:	alorscheider@dot.state.nc.us
Current Products:	The IEEE 1512 Family of Standards, which specifies message sets for incident management communication among Transportation Management Centers (including Intelligent Transportation Systems) and all other centers involved in incident management, such as public safety agencies.
Planned Products:	Technical standards, publications, and conferences, to present the best of the wireless and IT technology.
Additional Information:	Ed Rashba, Manager, New Technical Programs, IEEE 1512, 732-465-6449, e.rashba@ieee.org
Program Goals:	The IEEE 1512 promotes the engineering process of creating, developing, integrating, sharing, and applying knowledge about electro and information technologies and sciences for the benefit of humanity and the profession.

Sectors Addressed:

☑ *Law Enforcement*	☐ *Corrections*	☑ *EMS*	☑ *Military*
☐ *Courts*	☐ *Probat./Parole*	☑ *Emerg. Manag.*	☐ *Other*
☐ *Public Defender*	☑ *Fire Protection*	☑ *Transportation*	
☐ *Prosecution*	☑ *Public Works*	☑ *Utlities*	

Functional Capabilities:

Wireless Data

☑ Ability of users to quickly and transparently establish on-scene wireless data networks that function among data terminals located in on-scene vehicles and among data terminal carried by users into buildings, etc.

Wireless Data

☑ Ability of on-scene personnel to transparently exchange, as authorized, text, image, and/or video data with other on-site personnel, dispatchers, data resources, etc.

The primary purpose of the IEEE 1512 standards is standardizing the data elements and message sets for use in exchanging real-time information concerning Transportation Incident Management.

Wireless Data	
☑ Ability to protect the privacy of particular information according to applicable laws and statutes so that it can be accessed only by authorized personnel and data terminals.	The IEEE 1512 Standards were developed in such a manner that only authorized personnel and/or agencies may be privy to certain data elements and this is a local implementation choice, which needs to be determoined when developing the systems user requirements.
Wireless Data	
☑ Capability of high speed data transfer to allow fast exchange of text, image, and streaming video information.	IEEE 1512 does not deal with the security layer --- that is considered local implementation choice on level of system security deemed necessary
Wireless Data	
☑ Ability of transparent on-scene system access to multiple information systems regardless of differing data base system architectures and data formats.	
Wireless Data	
☑ Reliable system operational performance (including fault tolerant to individual system failures, redundant coverage from adjacent sites, full service during routine maintenance, and resistant to impact of catastrophic events).	Local implementation choice.
Information Systems	
☑ Ability to effectively and efficiently exchange data between agencies/jurisdictions, e.g., by employing common data representation structures and exchange formats and protocols.	This is its primary purpose.
Information Systems	
☑ Ability to rapidly access subject information at critical decision points from both field and base locations, including but not limited to information regarding identification (photos, fingerprints, etc.) and activity (criminal history, wants/warrants, reporting/contact history, etc.).	This is allowed with standard to access these data elements and exchange them from systems developed with other standards.
Information Systems	
☑ Ability to enter information once, then share and reuse that information among all entities that require it.	
Information Systems	
☑ Ability to query/access multiple data sources using one request that is routed to multiple entities simultaneously.	
Information Systems	
☑ Capability of standardized security, including functions and features that can be used to satisfy reasonable security requirements of any entity within a broader security framework.	Local implementation choice when implementing standard within a system.

Program/Organization:	**IEEE 1512**

Information Systems

☑ Ability to exchange information with Computer-Aided Dispatch (CAD) systems.	This is the primary purpose: to exchange data from CADs and transportation management systems.

Information Systems

☑ Capability of field photo scanning and image file distribution.	This is being done within the NYC deployment of IEEE 1512.

Information Systems

☑ Ability to have near-real-time distribution of text messages to multiple organizations responding to a large event.	It's the number one user requirement.

Information Systems

☑ Ability to access information related to hazardous materials, water sources, floor and building plans, utility maps, weather forecasts, topographic terrain, and other background data that may influence how public safety practitioners approach or conduct operations at an incident.	HazMat is standardized in IEEE 1512.3-2002. Exchange of weather, road condition, etc., is contained in IEEE 1512.1-2003.

Information Systems

☑ Ability to access medical/treatment records (both those required to ensure proper treatment of incident victims and/or prisoners and those records obtained under warrant).	IEEE P1512.2 tracks victims but does not contain any medical information.

Information Systems

☑ Ability to access current resource data (including personnel, equipment, materials, etc.) of multiple agencies/jurisdictions responding to a multi-agency/jurisdictional event by authorized users in the respective agencies/jurisdictions.	Asset information (including that of personnel) in IEEE P1512.2 and IEEE 1512.1-2003.

Program/Organization:	**IEEE 802**
Full Name:	Institute of Electrical and Electronics Engineers (IEEE), Committee 802
Agencies:	
Partnering Agencies / Orgs.:	Network experts from the industry, academia, and government (nationally and internationally)
Web Page:	http://www.ieee802.org
Contact Name:	Paul Nikolich
	IEEE 802 Chair
Contact Phone:	
Contact Email:	p.nikolich@ieee.org
Current Products:	
Planned Products:	Technical standards, publications, and conferences to present the best of the wired and wireless network technologies
Additional Information:	http://www.ieee.org Roger Marks marks@nist.gov Khaled Amer, AmerNet 949-522-1114 amer@amernet.net
Program Goals:	The IEEE 802 LAN/MAN Standards Committee develops Local Area Network standards and Metropolitan Area Network standards. The most widely used standards are for the Ethernet family, Token Ring, Wireless LAN, Bridging, and Virtual Bridged LANs. An individual working group provides the focus for each area. Three of the working groups that are commonly referred to when discussing wireless mobile data are: 802.11 -- Wireless Local Area Networks 802.15 -- Wireless Personal Area Networks 802.16 -- Wireless Metropolitan Area Networks. Ethernet family: 802.3 Token Ring: 802.5 Wireless LAN: 802.11 Bridging and Virtual Bridged LANs: 802.1 Resilient Packet Rings for MANs: 802.17

Sectors Addressed:				
☑ *Law Enforcement*	☐ *Corrections*	☑ *EMS*	☑ *Military*
☐ *Courts*	☐ *Probat./Parole*	☑ *Emerg. Manag.*	☑ *Other*
☐ *Public Defender*	☑ *Fire Protection*	☐ *Transportation*	*All*
☐ *Prosecution*	☑ *Public Works*	☑ *Utlities*	

Functional Capabilities:

Wireless Data

☑ Ability to initiate wireless data

The IEEE 802.16 Working Group has developed IEEE Standard 802.16 ("Air

communications by requiring the user to only enter (on his/her data terminal/radio) a user identification which authenticates and validates the user, registers and sets data resource capabilities for the user, and completes all radio network administration for the user's data communications with other members of the user's agency/jurisdiction and with other agencies/jurisdictions, as authorized.	Interface for Fixed Broadband Wireless Access Systems"), otherwise known as the WirelessMAN™ air interface for wireless metropolitan area networks. The group is currently developing the 802.16e enhancement for support of mobile terminals. The standard does not specify an entire systems, but the capabilities mentioned here would be readily supportable by the WirelessMAN air interface. IEEE 802.16 has been developed with hundreds of experts from around the world. Companies are currently developing implementations. Compliant products are expected in 2004. The primary applications are commercial and consumer, but features of the standard make it also appropriate for use in public safety.
Wireless Data	
☑ Ability of users to quickly and transparently establish on-scene wireless data networks that function among data terminals located in on-scene vehicles and among data terminal carried by users into buildings, etc.	IEEE Standard 802.16a (an element of IEEE Standard 802.16) specifies an optional mesh topology in which terminals may communicate directly with each other. This topology supplements the basic 802.16 point-to-multipoint architecture, in which terminals communicate with a base station.
Wireless Data	
☑ Ability of on-scene personnel to transparently exchange, as authorized, text, image, and/or video data with other on-site personnel, dispatchers, data resources, etc.	The 802.16 WirelessMAN air interface is well suited for this application because of its inherent support for Quality of Service. The design also allows for full support of voice and real-time video telephony.
Wireless Data	
☑ Ability to protect the privacy of particular information according to applicable laws and statutes so that it can be accessed only by authorized personnel and data terminals.	The 802.16 WirelessMAN air interface is well suited for this application. It includes thorough authentication originally designed to prevent commercial theft of service.
Wireless Data	
☑ Ability to ensure secure exchange of information.	The 802.16 WirelessMAN air interface is well suited for this application. It includes thorough security and encryption features designed to safeguard corporate data. Its security features are upgradeable for even stronger security
Wireless Data	
☑ Capability of high speed data transfer to allow fast exchange of text, image, and streaming video information.	The 802.16 air interface is designed for broadband data rates of tens of megabits per second. Because of its multimedia design, this data can be mixed with real-time transfers, like voice and video telephony.
Wireless Data	
☑ Ability of transparent on-scene system access to multiple information systems regardless of differing data base system architectures and data formats.	The 802.16 air interface supports connections to standard network layers, including Internet Protocol and ATM. It is independent of specific information system formats.
Wireless Data	
☑ Ability to remotely access a user's agency/jurisdiction data communications infrastructure when the user roams outside the radio coverage area of the user's agency/jurisdiction infrastructure.	This capability could be supported by the 802.16 air interface, particularly as roaming features are added through the ongoing 802.16e project.
Wireless Data	
☑ Reliable system operational performance (including fault tolerant to individual system failures, redundant coverage from adjacent sites, full service during routine maintenance, and resistant to impact of catastrophic events).	The 802.16 air interface includes adaptive link control. This means that, depending on the quality of the over-the-air channel, the physical modulation and coding methods are adjusted to ensure reliable communications with maximum transmission efficiency. The use of redundant base stations will improve resistance to catastrophic events.

Wireless Data

☑ Flexible and dynamic system administration (includes administration of on-scene wireless data networks).	Vendors who implement the standard will typically include remote systems management tools.

Program/Organization:	**INTELINK**
Full Name:	INTELINK Program
Agencies:	FBI, CIA, DEA, NSA, USSS, NRO
Partnering Agencies / Orgs.:	Federal agencies and authorized state and local agencies
Web Page:	
Contact Name:	Kenneth M. Ritchhart
Contact Phone:	202-324-7781
Contact Email:	kritchha@leo.gov
Current Products:	o A large, secure network o Standard mechanisms for indicating security level of a document
Planned Products:	
Additional Information:	Doug Ward Djward1080@yahoo.com 202-324-8954 Marcia Siedschlag Ice22blue@aol.com
Program Goals:	To link information in the various classified databases of the U.S. intelligence agencies (e.g., FBI, CIA, DEA, NSA, USSS, NRO) to facilitate communication and the sharing of documents and other resources

Sectors Addressed:	☑ ***Law Enforcement***	☐ ***Corrections***	☐ ***EMS***	☐ ***Military***
	☐ ***Courts***	☐ ***Probat./Parole***	☐ ***Emerg. Manag.***	☐ ***Other***
	☐ ***Public Defender***	☐ ***Fire Protection***	☐ ***Transportation***	
	☐ ***Prosecution***	☐ ***Public Works***	☐ ***Utlities***	

Program/Organization:	**IWN**
Full Name:	Integrated Wireless Network
Agencies:	U.S. Department of Justice U.S. Department of Homeland Security
Partnering Agencies / Orgs.:	Agencies in the Departments of Treasury, Justice, and Homeland Security
Web Page:	http://www.usdoj.gov/
Contact Name:	Michael Duffy
	Deputy CIO for e-Government DoJ Information Resources Management
Contact Phone:	202-305-4568
Contact Email:	michael.duffy@usdoj.gov
Current Products:	o A system engineering and implementation plan study for nationwide IWN o A pilot system in the Northwest Region
Planned Products:	
Additional Information:	Tim Ritter, DOJ Integrated Wireless Network Project Manager 703-322-1661
Program Goals:	o to acquire integration services and equipment to replace aging systems o to meet new NTIA narrowband mandates o to improve interoperability among Federal, state, and local law enforcement agencies, and o to achieve economies of scale in acquisition and operations

Sectors Addressed:	☑ ***Law Enforcement***	☑ ***Corrections***	☐ ***EMS***	☐ ***Military***
	☑ ***Courts***	☐ ***Probat./Parole***	☑ ***Emerg. Manag.***	☐ ***Other***
	☐ ***Public Defender***	☐ ***Fire Protection***	☐ ***Transportation***	
	☐ ***Prosecution***	☐ ***Public Works***	☐ ***Utlities***	

Functional Capabilities:

Wireless Voice

☑ Ability to initiate wireless voice communications by requiring the user to only enter (on his/her radio) a user identification which authenticates and validates the user, registers and sets talk groups/capabilities for the user, and completes all radio network administration for the user's voice communications with other members of the user's agency/jurisdiction and with other agencies/jurisdictions, as authorized.

The Integrated Wireless Network (IWN) is based on VHF, P.25, trunked architecture with VoIP connectivity. User devices (subscribers) are P.25 compliant radios with user identification capabilities (radio ID) associated with each radio. Each radio will be programmed to support the user's needs to include: talk groups, functionality, OTAR, OTAP, and encryption algorithms. At this time, the system will not incorporate the use of downloading user profiles from the network based on a user entered ID or password.

Program/Organization:	**IWN**

Wireless Voice

☑ Ability for users to transparently communicate, as authorized, with other members of the agency/jurisdiction on a unit-to-group (one-to-many) basis and a unit-to-unit (one-to-one) basis.	IWN incorporates P.25 trunking features such as unit-to-group (one-to-many) basis and a unit-to-unit (one-to-one) communications.

Wireless Voice

☑ Ability of the agency/jurisdiction to administer the priority for voice communications of particular users and particular applications (such as task force operations, incidents, etc.).	IWN incorporates priority queuing and 'ruthless preemption' for voice communications based on user requirements.

Wireless Voice

☑ Ability to communicate an emergency voice message and/or signal which has priority over other voice communications.	Priority emergency alarm/call function and alarm is provided.

Wireless Voice

☑ Ability to have secure voice communications.	End-to-end AES encryption is provided.

Wireless Voice

☑ Ability for users to transparently communicate, as authorized, among multiple agencies/jurisdictions some of which may use different technologies, infrastructures and/or frequency bands.	Interoperations solutions that allow transparent communications are included in the IWN design. Solutions allow 'connection' of disparate systems through a variety of mechanisms (gateways, cross-banding, etc.).

Wireless Voice

☑ Ability to remotely access a user's agency/jurisdiction voice communications infrastructure when the user roams outside the radio coverage area of the user's agency/jurisdiction wireless infrastructure.	IWN is a nation-wide trunked radio system that allows nation-wide roaming (as required).

Wireless Voice

☑ Ability to effectively initiate and sustain flexible and dynamic system administration (includes administration of talk groups, emergency alerts, networks, and channels for mutual aid).	IWN architecture includes centralized system management and administration.

Wireless Voice

☑ Ability to sustain highly reliable system performance across interconnected systems (including tolerance to individual system failures, redundant coverage from adjacent sites, resistance to impact of catastrophic events, etc).	System reliability is provided in the form of fault tolerant or redundant system components and development of robust sites. Redundant coverage is not typically a design criterion due to expense.

Wireless Voice

☑ Ability to remotely (over-the-air) reprogram a user's radios and/or modify a user's encryption keys and/or modify a radio's waveforms.	IWN includes both OTAR and OTAP.

Wireless Voice

☑ Ability to provide state-wide (county-wide) signal coverage to vehicular/mobile radios on highways and at street level for state (county) agencies, to provide city-wide signal coverage to portable/handheld radios on the street and within buildings for city agencies, and to provide direct communications between user radios when there is no wireless infrastructure to support communications (such in some rural areas, underground parking garages, and inside some buildings).	IWN, a high-level design criterion, includes: handheld street-level coverage in urban areas, mobile coverage 5 miles on either side of major highways and interstates, portable coverage 5 miles from U.S. land borders, tribal lands, and in-building coverage as required (airports, ports-of-entry, U.S. courthouses, etc.). Actual coverage for IWN 'areas' is based on coverage requirements for that specific area.

Wireless Data

☑ Ability to initiate wireless data communications by requiring the user to only enter (on his/her data terminal/radio) a user identification which authenticates and validates the user, registers and sets data resource capabilities for the user, and completes all radio network administration for the user's data communications with other members of the user's agency/jurisdiction and with other agencies/jurisdictions, as authorized.	The Integrated Wireless Network (IWN) is based on VHF, P.25, trunked architecture with VoIP connectivity. User devices (subscribers) are P.25 compliant radios with user identification capabilities (radio ID) associated with each radio. Each radio will be programmed to support the user's needs to include: talk groups, functionality, OTAR, OTAP, and encryption algorithms. At this time, the system will not incorporate the use of downloading user profiles from the network based on a user entered ID or password. Data in the form of OTAR, text messaging, access to specific data applications (NCIC, etc.) is provided. High-speed data applications services are typically provided by commercial services.

Wireless Data

☑ Ability to protect the privacy of particular information according to applicable laws and statutes so that it can be accessed only by authorized personnel and data terminals.	Database access requires user authentication and system utilizes end-to-end AES encryption

Wireless Data

☑ Ability to ensure secure exchange of information.	End-to-end AES encryption is provided.

Wireless Data

☑ Capability of high speed data transfer to allow fast exchange of text, image, and streaming video information.	High-speed data transfer is typically provided by commercial services.

Wireless Data

☑ Ability to remotely access a user's agency/jurisdiction data communications infrastructure when the user roams outside the radio coverage area of the user's agency/jurisdiction infrastructure.	IWN is a nation-wide trunked radio system that allows nation-wide roaming (as required).

Wireless Data

☑ Reliable system operational performance (including fault tolerant to individual system failures, redundant coverage from adjacent sites, full service during routine maintenance, and resistant to impact of catastrophic events).	System reliability is provided in the form of fault tolerant or redundant system components and development of robust sites. Redundant coverage is not typically a design criterion due to expense.

Wireless Data

☑ Flexible and dynamic system administration (includes administration of on-scene wireless data networks).	IWN architecture includes centralized system management and administration.

Program/Organization:	**IWN**

Information Systems

☑ Ability to effectively and efficiently exchange data between agencies/jurisdictions, e.g., by employing common data representation structures and exchange formats and protocols.	IWN infrastructure utilizes packet based IP network protocol.

Information Systems

☑ Ability to rapidly access subject information at critical decision points from both field and base locations, including but not limited to information regarding identification (photos, fingerprints, etc.) and activity (criminal history, wants/warrants, reporting/contact history, etc.).	Access to subject information that can be accessed with low-speed connections is supported by the IWN. Access to subject information that requires high-speed connectivity is supported by IWN user access to communications center support staff (who have high-speed database access).

Information Systems

☑ Capability of standardized security, including functions and features that can be used to satisfy reasonable security requirements of any entity within a broader security framework.	IWN incorporates security features that satisfy system certification and acceptance requirements.

Information Systems

☑ Ability to have near-real-time distribution of text messages to multiple organizations responding to a large event.	IWN will support real-time distribution of text messages. Testing with FBI-Dallas Emergency Response Network will occur in mid-2003 timeframe.

Information Systems

☑ Ability to access information related to hazardous materials, water sources, floor and building plans, utility maps, weather forecasts, topographic terrain, and other background data that may influence how public safety practitioners approach or conduct operations at an incident.	Access to subject information that can be accessed with low-speed connections is supported by the IWN. Access to subject information that requires high-speed connectivity is supported by IWN user access to communications center support staff (who have high-speed database access).

Information Systems

☑ Ability to access information regarding pending investigation/litigation of a particular subject.	Access to subject information that can be accessed with low-speed connections is supported by the IWN. Access to subject information that requires high-speed connectivity is supported by IWN user access to communications center support staff (who have high-speed database access).

Program/Organization:	**JTRS JPO**
Full Name:	Joint Tactical Radio System Joint Program Office
Agencies:	U.S. Department of Defense
Partnering Agencies / Orgs.:	Office of the Secretary of Defense (OSD), U.S. Army, U.S. Air Force, U.S. Navy, U.S. Marine Corps
Web Page:	http://jtrs.army.mil
Contact Name:	Maj David Herring, USAF
Contact Phone:	703-588-1056
Contact Email:	david.herring@hqda.army.mil
Current Products:	
Planned Products:	A family of affordable, high-capacity tactical radios to provide interoperable line-of-sight/beyond line-of-sight command, control, communications, computers, and intelligence capabilities to the warfighters.
Additional Information:	
Program Goals:	1. To acquire a family of affordable, high-capacity tactical radios that provide interoperable line-of-sight/beyond line-of-sight command, control, communications, computers, and intelligence capabilities. 2. To develop a family of software programmable radios designed around a Software Communications Architecture (SCA) that provide for mission reconfigurability and system reprogramability. 3. To develop with industry an SCA for SDRs, which promotes waveform portability and provides bridging and simulcast capabilities. 4. To provide seamless reliable multi-channel voice, data, imagery, and video interoperable network-centric communications, and to integrate legacy systems. 5. To enable (with next-generation SDR technology) technology insertion. 6. To achieve interoperability with joint and international coalition partners. 7. To achieve interoperability with the 1st responder community.

Sectors Addressed:	☑ ***Law Enforcement***	☐ ***Corrections***	☑ ***EMS***	☑ ***Military***
	☐ ***Courts***	☐ ***Probat./Parole***	☑ ***Emerg. Manag.***	☐ ***Other***
	☐ ***Public Defender***	☑ ***Fire Protection***	☐ ***Transportation***	
	☐ ***Prosecution***	☐ ***Public Works***	☐ ***Utlities***	

Functional Capabilities:

Wireless Voice

☑ Ability for users to transparently communicate, as authorized, with other members of the agency/jurisdiction on a unit-to-group (one-to-many) basis and a unit-to-	Software Defined Radio (SDR) technology using the JTRS open standard Software Communications Architecture (SCA) is used to provide this capability. A software version of the APCO Project 25 waveform will also support this capability for non-DoD users.

unit (one-to-one) basis.

Wireless Voice

☑ Ability of the agency/jurisdiction to administer the priority for voice communications of particular users and particular applications (such as task force operations, incidents, etc.).	Software Defined Radio (SDR) technology using the JTRS open standard Software Communications Architecture (SCA) is used to provide this capability for DoD only using the new Wideband Networking Waveform (WNW).

Wireless Voice

☑ Ability to communicate an emergency voice message and/or signal which has priority over other voice communications.	Software Defined Radio (SDR) technology using the JTRS open standard Software Communications Architecture (SCA) is used to provide this capability for DoD only using the new Wideband Networking Waveform (WNW).

Wireless Voice

☑ Ability to have secure voice communications.	Software Defined Radio (SDR) technology using the JTRS open standard Software Communications Architecture (SCA) is used to provide this capability. The JTRS SCA supports communications security and programmable cryptographic capabilities up through Type 1 Security for DoD requirements.

Wireless Voice

☑ Ability for users to transparently communicate, as authorized, among multiple agencies/jurisdictions some of which may use different technologies, infrastructures and/or frequency bands.	Software Defined Radio (SDR) technology using the JTRS open standard Software Communications Architecture (SCA) is used to provide this capability. The SCA supports portable waveforms. Therefore one radio can use many different waveforms allowing it to interoperate with many different disparate communications systems.

Wireless Voice

☑ Ability to effectively initiate and sustain flexible and dynamic system administration (includes administration of talk groups, emergency alerts, networks, and channels for mutual aid).	Software Defined Radio (SDR) technology using the JTRS open standard Software Communications Architecture (SCA) is used to provide this capability for DoD using the new Wideband Networking Waveform (WNW). To a lesser extent this capability can be provided to civilian 1st responders using the APCO Project 25 waveform.

Wireless Voice

☑ Ability to remotely (over-the-air) reprogram a user's radios and/or modify a user's encryption keys and/or modify a radio's waveforms.	Software Defined Radio (SDR) technology using the JTRS open standard Software Communications Architecture (SCA) is used to provide this capability. JTRS is specifically designed to provide capability for over the air (OTA) rekeying and OTA reprogramming to include changing waveforms.

Wireless Data

☑ Ability of users to quickly and transparently establish on-scene wireless data networks that function among data terminals located in on-scene vehicles and among data terminal carried by users into buildings, etc.	Software Defined Radio (SDR) technology using the JTRS open standard Software Communications Architecture (SCA) is used to provide this capability for DoD using the new Wideband Networking Waveform (WNW). The WNW is designed to provide the capability of self-forming, self-healing ad hoc networks on the battlefield.

Wireless Data

☑ Ability of on-scene personnel to transparently exchange, as authorized, text, image, and/or video data with other on-site personnel, dispatchers, data resources, etc.	Software Defined Radio (SDR) technology using the JTRS open standard Software Communications Architecture (SCA) is used to provide this capability for DoD using the new Wideband Networking Waveform (WNW).

Wireless Data

☑ Ability to protect the privacy of particular information according to applicable laws and statutes so that it can be accessed only by authorized personnel and data terminals.	Software Defined Radio (SDR) technology using the JTRS open standard Software Communications Architecture (SCA) is used to provide this capability. The JTRS SCA and its multi-channel, multi-mode operation capability supports communications security and programmable cryptographic capabilities up through Type 1 Security (for DoD requirements) using multiple single levels of security. This capability also applies to voice communication.

Program/Organization:	**JTRS JPO**

Wireless Data

☑ Ability to ensure secure exchange of information.	Software Defined Radio (SDR) technology using the JTRS open standard Software Communications Architecture (SCA) is used to provide this capability for DoD. The JTRS SCA supports communications security and programmable cryptographic capabilities up through Type 1 Security for DoD requirements.

Wireless Data

☑ Capability of high speed data transfer to allow fast exchange of text, image, and streaming video information.	Software Defined Radio (SDR) technology using the JTRS open standard Software Communications Architecture (SCA) is used to provide this capability for DoD using the new Wideband Networking Waveform (WNW).

Wireless Data

☑ Flexible and dynamic system administration (includes administration of on-scene wireless data networks).	Software Defined Radio (SDR) technology using the JTRS open standard Software Communications Architecture (SCA) is used to provide this capability for DoD using the new Wideband Networking Waveform (WNW).

Information Systems

☑ Capability of standardized security, including functions and features that can be used to satisfy reasonable security requirements of any entity within a broader security framework.	Software Defined Radio (SDR) technology using the JTRS open standard Software Communications Architecture (SCA) is used to provide this capability for DoD. The JTRS SCA and its multi-channel, multi-mode operation capability supports communications security and programmable cryptographic capabilities up through Type 1 Security for DoD requirements using multiple single levels of security. This capability also applies to voice communication.

Information Systems

☑ Ability to have near-real-time distribution of text messages to multiple organizations responding to a large event.	Software Defined Radio (SDR) technology using the JTRS open standard Software Communications Architecture (SCA) is used to provide this capability for DoD using the new Wideband Networking Waveform (WNW). WNW allows for creation for the tactical internet where this kind of information can be shared.

Program/Organization:	**Major City Chiefs Association**
Full Name:	Major City Chiefs Association
Agencies:	United States and Canadian Association
Partnering Agencies / Orgs.:	Law enforcement executives in cities of greater than 1.5 million population, and departments that employ more than 1,000 law enforcement officers.
Web Page:	http://www.neiassociates.org/about.htm
Contact Name:	Harlin McEwen
	Communications Advisor
Contact Phone:	607-257-1522
Contact Email:	ChiefHRM@leo.gov
Current Products:	
Planned Products:	
Additional Information:	Additional contacts: Thomas Frazier, MCC Executive Director 410-433-8909 tfrazier@attach.net
Program Goals:	o To address problems unique to large police organizations o To provide training for administrators of large LE organizations

Sectors Addressed:	☑ ***Law Enforcement***	☐ ***Corrections***	☐ ***EMS***	☐ ***Military***
	☐ ***Courts***	☐ ***Probat./Parole***	☐ ***Emerg. Manag.***	☐ ***Other***
	☐ ***Public Defender***	☐ ***Fire Protection***	☐ ***Transportation***	
	☐ ***Prosecution***	☐ ***Public Works***	☐ ***Utlities***	

Program/Organization:	**MCSA**
Full Name:	Major County Sheriffs' Association
Agencies:	
Partnering Agencies / Orgs.:	
Web Page:	
Contact Name:	Harlin McEwen
	Communications Advisor, Law Enforcement and Corrections
Contact Phone:	607-257-1522
Contact Email:	ChiefHRM@leo.gov

Current Products:	o A law-enforcement, information gathering resource o Technical assistance and research entities (in conjunction with the National Sheriff's Assocation, the Major Cities Chiefs, the Federal Bureau of Investigation Training Division, the National Executive Institute, and other private or public research entities)
Planned Products:	
Additional Information:	Kevin Beary, MCSA President Sheriff of Orange County 2400 West 33rd Street Orlando, FL 407-836-3700 ocso@magicnet.net Margo Frasier, Vice President Joseph Wolfinger, Executive Director 703-684-7114 Joe.Wolfinger@mpri.l-3com.com
Program Goals:	o To promote greater understanding of law enforcement strategies to address future problems and identify law-enforcement challenges o To advance legislative issues that will enhance community safety o To promote the development of innovative education, prevention, and enforcement strategies and programs o To provide a forum in which to share ideas, concepts, and resources

Sectors Addressed:	☑ *Law Enforcement*	☑ *Corrections*	☐ *EMS*	☐ *Military*
	☐ *Courts*	☐ *Probat./Parole*	☐ *Emerg. Manag.*	☐ *Other*
	☐ *Public Defender*	☐ *Fire Protection*	☐ *Transportation*	
	☐ *Prosecution*	☐ *Public Works*	☐ *Utlities*	

Program/Organization:	**NASA's Earth Alert Program**
Full Name:	NASA's Earth Alert Program
Agencies:	NASA
Partnering Agencies / Orgs.:	FEMA, National Weather Service, Maryland Emergency Management Admin., Maryland National Guard
Web Page:	http://www.3eti.com
Contact Name:	Fred Schamann
	Earth Alert Program Manager
Contact Phone:	301-286-7039
Contact Email:	fredrick.g.schamann@nasa.gov

Current Products:	o Geo-referenced communications and messaging service o Wireless clients o Custom applications menus o Weather feed services o Data base interfaces o Geographic Information System (GIS) services o Asset tracking o Damage assessment forms/services/reports o First responder messaging o Alert event messaging
Planned Products:	o All-Hazard Allerting and First Responder support o Homeland Defense applications o Military/National Guard base applications
Additional Information:	Chris Sluss, Aeptec/3eti 301-670-6779
Program Goals:	o Development of a wireless warning and emergency management support system for all hazards o Transfer the NASA's Earth Alert technology for commercial applications such as roadside service, transportation tracking, leisure services, etc., and o Support/transfer the local/regional emergency management community with NASA-developed/supported technologies

Sectors Addressed:	☑ ***Law Enforcement***	☑ ***Corrections***	☑ ***EMS***	☑ ***Military***
	☐ ***Courts***	☐ ***Probat./Parole***	☑ ***Emerg. Manag.***	☑ ***Other***
	☐ ***Public Defender***	☑ ***Fire Protection***	☑ ***Transportation***	***CDC***
	☐ ***Prosecution***	☑ ***Public Works***	☑ ***Utlities***	

Functional Capabilities:

Wireless Data

☑ Ability to initiate wireless data communications by requiring the user to only

Based on feedback from emergency management organizations and AEPTEC research we have determined that further expansion of the use of consumer

enter (on his/her data terminal/radio) a user identification which authenticates and validates the user, registers and sets data resource capabilities for the user, and completes all radio network administration for the user's data communications with other members of the user's agency/jurisdiction and with other agencies/jurisdictions, as authorized.	wireless networks and devices was needed. Many governments utilize Nextel wireless devices and capabilities. Nextel i88 phones have the capabilities to provide wireless voice, data service, and GPS capabilities needed for providing location information. Since many government agencies do not have the capabilities or funding to build all the necessary components of a wireless data solution AEPTEC will offer the solution as a subscription service or as a direct sale to accommodate small or large prospects. AEPTEC will utilize the GPS capabilities in the Nextel I88 phone. The Nextel service is also a preferred service of contractors and other commercial support mechanisms put in place during times of crisis. The solution will most likely include but not be limited to enhancing access through the web to damage assessment information, disaster mitigation and assessment on the Nextel i88 phone, it will also include further features such as directions to critical incidents, support capabilities and shelter availability (hotels, government buildings). A weather feed will enable requests for location specific updates to a Nextel phone and to enable emergency management personnel to stay up to date on weather progression. The solution will also enable command center personnel web tracking screen access. Some of the wireless data service providers supported: - Nextel Packet Data - CDPD with EarthLink - Aeris Microburst - SMS Messaging - Verizon - Sprint - Cingular - Satelite
Wireless Data	
☑ Ability of users to quickly and transparently establish on-scene wireless data networks that function among data terminals located in on-scene vehicles and among data terminal carried by users into buildings, etc.	802.11 FIPS 140 network pending. Already deployed on Navy ships and bases. Working on a mobile deployed system that will have portable sensor kits and video capabilities. Plus an uplink to send data back to a central location.
Wireless Data	
☑ Ability of on-scene personnel to transparently exchange, as authorized, text, image, and/or video data with other on-site personnel, dispatchers, data resources, etc.	802.11 FIPS 140 network pending. Already deployed on Navy ships and bases. Working on a mobile deployed system that will have portable sensor kits and video capabilities. Plus an uplink to send data back to a central location.
Wireless Data	
☑ Ability to protect the privacy of particular information according to applicable laws and statutes so that it can be accessed only by authorized personnel and data terminals.	802.11 FIPS 140 network pending. Already deployed on Navy ships and bases. Working on a mobile deployed system that will have portable sensor kits and video capabilities. Plus an uplink to send data back to a central location.
Wireless Data	
☑ Ability to ensure secure exchange of information.	Utilizing Nextel wide area networks with AES encryption. 802.11 FIPS 140 network pending. Already deployed on Navy ships and bases. Working on a mobile deployed system that will have portable sensor kits and video capabilities. Plus an uplink to send data back to a central location.
Wireless Data	
☑ Capability of high speed data transfer to allow fast exchange of text, image, and streaming video information.	802.11 FIPS 140 network pending. Already deployed on Navy ships and bases. Working on a mobile deployed system that will have portable sensor kits and video capabilities. Plus an uplink to send data back to a central location.

Wireless Data

☑ Ability of transparent on-scene system access to multiple information systems regardless of differing data base system architectures and data formats.

Utilizing a wide area Nextel network we are able to process data two-way through the web to multiple locations.

Wireless Data

☑ Ability to remotely access a user's agency/jurisdiction data communications infrastructure when the user roams outside the radio coverage area of the user's agency/jurisdiction infrastructure.

By using a satellite uplink and a laptop PC we can dock or wireless network in many different users.

Wireless Data

☑ Reliable system operational performance (including fault tolerant to individual system failures, redundant coverage from adjacent sites, full service during routine maintenance, and resistant to impact of catastrophic events).

By being flexible in the receipt and delivery of information we can access information from many wireless networks and satellite solutions, plus we can revert to land line when all else fails.

Wireless Data

☑ Flexible and dynamic system administration (includes administration of on-scene wireless data networks).

802.11 FIPS 140 network pending. Already deployed on Navy ships and bases. Working on a mobile deployed system that will have portable sensor kits and video capabilities. Plus an uplink to send data back to a central location.

Information Systems

☑ Ability to effectively and efficiently exchange data between agencies/jurisdictions, e.g., by employing common data representation structures and exchange formats and protocols.

See previous Wireless Data information. We can be placed behind a firewall or we can be a web based subscription service depending on the needs of the customer.

Information Systems

☑ Ability to rapidly access subject information at critical decision points from both field and base locations, including but not limited to information regarding identification (photos, fingerprints, etc.) and activity (criminal history, wants/warrants, reporting/contact history, etc.).

We use the solution to report many types of information and display in the text format or in GIS format, depending on the needs of the customer.

Information Systems

☑ Ability to enter information once, then share and reuse that information among all entities that require it.

With our web based design we allow local government to gain access to the latest technology and then we can role that data up to the state and Federal levels. Depending on the user profile access is available. The data can be used in any way they feel is appropriate.

Information Systems

☑ Ability to query/access multiple data sources using one request that is routed to multiple entities simultaneously.

The system provides for multiple entities to access and manipulate data based on the profile. We can take information feeds and process them logically by location or by the profile.

Information Systems

☑ Capability of standardized security, including functions and features that can be used to satisfy reasonable security requirements of any entity within a broader security framework.

Current solutions have password protection and security sufficient for use by government agencies, and we have the capability to increase the level of security depending on the requirements.

Information Systems

☑ Ability to exchange information with Computer-Aided Dispatch (CAD) systems.

We also connect location information from a phone equipped with GPS technology through a PBX so the Call Center Operator can see the location of the caller. We also allow the Call Center Operator to see persons on a screen and then either call the person or send a text message or an alert.

Information Systems

☑ Capability of field photo scanning and image file distribution.

Future capability for the wide area Nextel solution and a solution already deployed with the 802.11 solution.

Information Systems

☑ Ability to have near-real-time distribution of text messages to multiple organizations responding to a large event.

We have the ability to do both real time and near real time solutions. We currently can track personnel in a real time manner.

Information Systems

☑ Ability to access information related to hazardous materials, water sources, floor and building plans, utility maps, weather forecasts, topographic terrain, and other background data that may influence how public safety practitioners approach or conduct operations at an incident.

Our solution is limited only by the needs of our customers and their budget.

Program/Organization:	**NASCIO**
Full Name:	National Association of State Chief Information Officers
Agencies:	National Association
Partnering Agencies / Orgs.:	Executive-level CIOs of all 50 states, 6 territories and the District of Columbia; Federal, local, non-profit, academic, and private sector representatives with interest in and/or who provide products and services to state information technology organizations may also participate.
Web Page:	http://www.nascio.org
Contact Name:	Gerry Wethington President
Contact Phone:	573-526-7741
Contact Email:	wethig@mail.oit.state.mo.us
Current Products:	Conferences -- Mid-Year (Spring) and Annual (Fall) Publications -- Digital Government Compendium, Enterprise Architecture Development Tool Kit, State IT Best Practice Guides, Issue & Policy Reports, White Papers Awards -- Recognition (State IT Best Practices) Awards, National Technology Champion Award Committees/Working Groups -- Cybersecurity, Enterprise Architecture, Homeland Security, Partnerships, Privacy, Strategic IT Business and Services, Wireless and Spectrum Management
Planned Products:	NASCIO's Architecture Working Group is working in partnership with the U.S. Department of Justice, Office of Justice Programs (OJP) to institutionalize enterprise architecture in state and local government. The Architecture Program has produced deliverables designed to aid government entities as they build a technology adaptive enterprise through implementation of an architecture that is responsive to business processes and the supporting technology.
Additional Information:	Elizabeth Miller NASCIO Executive Director 167 West Main Street, Suite 600 Lexington, KY 40507-1324 859-514-9171 emiller@amrinc.net Jack Gallt NASCIO Wireless Issues Coordinator 167 West Main Street, Suite 600 Lexington, KY 40507-1324 859-514-9187 jgallt@amrinc.net
Program Goals:	NASCIO's mission is to serve as the primary source of information on issues, trends, and legislation affecting state IT initiatives and policies. NASCIO shapes national IT policy through collaborative partnerships, information sharing, and knowledge transfer across jurisdictional and functional boundaries.

Program/Organization:	**NASCIO**			
Sectors Addressed:	☑ *Law Enforcement*	☑ *Corrections*	☑ *EMS*	☐ *Military*
	☑ *Courts*	☑ *Probat./Parole*	☑ *Emerg. Manag.*	☐ *Other*
	☑ *Public Defender*	☑ *Fire Protection*	☑ *Transportation*	
	☑ *Prosecution*	☑ *Public Works*	☑ *Utlities*	

Program/Organization:	**NASTD**
Full Name:	The National Association of State Telecommunications Directors
Agencies:	National Association
Partnering Agencies / Orgs.:	Telecommunications and technology professionals serving state government
Web Page:	http://www.nastd.org
Contact Name:	Hale Irwin
	NASTD President
Contact Phone:	859-244-8186
Contact Email:	hale.irwin@state.vt.us
Current Products:	1. STARS (State Archives and Research Service Database) available on www.http://stars.csg.org/Excite/getting_started2.html 2. Reports/Publications, web pages, newsletters, resource library, results of surveys, state profiles 3. Open fora, Conferences
Planned Products:	
Additional Information:	Pam Johnson, NASTD Administration Manager at (859) 244-8184 or pjohnson@csg.org.
Program Goals:	1. To remain informed regarding telecom technology advances 2. To remain current in knowledge about IT and wireless security measures. NASTD, the Association for Telecommunications and Technology Professionals Serving State Government, is a member-driven organization whose purpose is to advance and promote the effective use of telecommunications technology and services to improve the operation of state government.

Sectors Addressed:			
☑ ***Law Enforcement***	☐ ***Corrections***	☑ ***EMS***	☐ ***Military***
☐ ***Courts***	☐ ***Probat./Parole***	☑ ***Emerg. Manag.***	☐ ***Other***
☐ ***Public Defender***	☑ ***Fire Protection***	☑ ***Transportation***	
☐ ***Prosecution***	☑ ***Public Works***	☐ ***Utlities***	

Program/Organization:	**NCJA**
Full Name:	National Criminal Justice Association
Agencies:	National Association
Partnering Agencies / Orgs.:	Representatives from the Federal, Tribal, State, and local LE officials. Its members represent all facets of the criminal and juvenile justice community, from law enforcement, corrections, prosecution, defense, courts, victim-witness services and educational institutions to federal, state and local elected officials.
Web Page:	http://www.ncja.org/
Contact Name:	Cabell C. Cropper Executive Director
Contact Phone:	202-628-8550 x101
Contact Email:	ccropper@ncja.org
Current Products:	o Integrated Justice Technology for Decision Makers Seminar o Technical Courses: XML for Integrated Justice; Security Strategies for Integrated Justice; and Multi-Jurisdictional Information Sharing and Data Mining for Integrated Justice
Planned Products:	National Forum 2003: Partnerships with Purpose: Visions for the Future of Public Safety July 19 - 23, 2003. This Forum represents a collaboration among the National Criminal Justice Association (NCJA), the Industry Working Group (IWG), the Integrated Justice Information Systems (IJIS) Institute, and the Justice Information Sharing Professionals (JISP). These groups represent policymakers and practitioners from state, tribal, and local governments as well as private enterprise providers of products and services to the justice enterprise. The meeting will explore how building new relationships, such as public/private partnerships and regional collaborations, will advance public safety, criminal justice, and information sharing.
Additional Information:	Further contact information: Mr. Cabell C. Cropper 202/628-8550 National Criminal Justice Association 720 7th Street, NW, Third Floor Washington, D.C. 20001-3716 Phone: 202-628-8550 Email: info@ncja.org
Program Goals:	Fosters the development of state, tribal, and local justice systems that 1. Enhance public safety 2. Prevent or reduce the harmful effects of criminal behavior on victims, individuals and communities; 3. Adjudicate defendants and sanction offenders fairly and justly; and 4. Use their resources effectively and efficiently. As a partner in the nation's capital, the NCJA 5. Focuses state, tribal, local, and Federal governments on the needs of the criminal and juvenile justice systems; 6. Represents state, tribal, and local criminal and juvenile justice concerns to the Federal government; 7. Provides support to the nation's governors on criminal and juvenile justice policy development;

Program/Organization:	**NCJA**
	8. Supports public safety through effective law enforcement and criminal and juvenile justice practices, as well as coordination of education, community, and social service systems; 9. Serves as a catalyst for careful consideration and promotion of effective and efficient criminal and juvenile justice system policies and practices.

Sectors Addressed:				
☑ *Law Enforcement*	☑ *Corrections*	☐ *EMS*	☐ *Military*
☑ *Courts*	☑ *Probat./Parole*	☐ *Emerg. Manag.*	☐ *Other*
☑ *Public Defender*	☐ *Fire Protection*	☐ *Transportation*	
☑ *Prosecution*	☐ *Public Works*	☐ *Utlities*	

Program/Organization:	**NCS**
Full Name:	National Communications System
Agencies:	Department of Homeland Security, Information Analysis & Infrastructure Protection Directorate
Partnering Agencies / Orgs.:	
Web Page:	www.ncs.gov
Contact Name:	Gary Amato
	Deputy Chief, Technology and Programs, DHS-NCS
Contact Phone:	703-607-6120
Contact Email:	amatog@ncs.gov
Current Products:	o Government Emergency Telephone Service (GETS), which provides emergency access and priority processing in the local and long distance segments of the Public Switched Network (PSN). It is intended to be used in an emergency or crisis situation during which the probability of completing a call over normal or other alternate telecommunication means has significantly decreased o The Wireless Priority System (WPS) was implemented in areas of the eastern United States in January 2003.
Planned Products:	
Additional Information:	
Program Goals:	National Security and Emergency Preparedness (NS/EP)

Sectors Addressed:	☑ *Law Enforcement*	☐ *Corrections*	☑ *EMS*	☑ *Military*
	☐ *Courts*	☐ *Probat./Parole*	☑ *Emerg. Manag.*	☑ *Other*
	☐ *Public Defender*	☑ *Fire Protection*	☑ *Transportation*	*EOP*
	☐ *Prosecution*	☑ *Public Works*	☑ *Utlities*	

Functional Capabilities:

Wireless Voice

☑ Ability to initiate wireless voice communications by requiring the user to only enter (on his/her radio) a user identification which authenticates and validates the user, registers and sets talk groups/capabilities for the user, and completes all radio network administration for the user's voice communications with other members of the user's agency/jurisdiction and with other agencies/jurisdictions, as authorized.	Wireless Priority Service (WPS) gives authorized users priority access on commercial wireless networks.

Program/Organization:	**NCS**

Wireless Voice

☑ Ability for users to transparently communicate, as authorized, with other members of the agency/jurisdiction on a unit-to-group (one-to-many) basis and a unit-to-unit (one-to-one) basis.	Wireless Priority Service is based upon a priority queuing scheme that allows key users access to a radio channel during congested times within publicly maintained/operated wireless networks, e.g., cellular infrastructure.

Wireless Voice

☑ Ability of the agency/jurisdiction to administer the priority for voice communications of particular users and particular applications (such as task force operations, incidents, etc.).	This is a key requirement. The ability to adjudicate the level of priority assigned to any user/user groups must be centrally coordinated.

Wireless Voice

☑ Ability to communicate an emergency voice message and/or signal which has priority over other voice communications.	Priority over other users within the community, also.

Wireless Voice

☑ Ability to have secure voice communications.	For certain users yes. NSA-approved secure sleeves in use.

Wireless Voice

☑ Ability for users to transparently communicate, as authorized, among multiple agencies/jurisdictions some of which may use different technologies, infrastructures and/or frequency bands.	Interoperability among technical systems as well as operational/procedural ones.

Wireless Voice

☑ Ability to remotely access a user's agency/jurisdiction voice communications infrastructure when the user roams outside the radio coverage area of the user's agency/jurisdiction wireless infrastructure.	

Wireless Voice

☑ Ability to provide state-wide (county-wide) signal coverage to vehicular/mobile radios on highways and at street level for state (county) agencies, to provide city-wide signal coverage to portable/handheld radios on the street and within buildings for city agencies, and to provide direct communications between user radios when there is no wireless infrastructure to support communications (such in some rural areas, underground parking garages, and inside some buildings).	No significant work here other than supporting growth and build-out of existing infrastructure and support to spectrum allocation issues.

Wireless Data

☑ Ability to initiate wireless data communications by requiring the user to only enter (on his/her data terminal/radio) a user identification which authenticates and validates the user, registers and sets data resource capabilities for the user, and completes all radio network administration for the user's data communications with other members of the user's agency/jurisdiction and with other agencies/jurisdictions, as authorized.

Wireless Priority Service (WPS) gives authorized users priority access on commercial wireless networks.

Wireless Data

☑ Ability of users to quickly and transparently establish on-scene wireless data networks that function among data terminals located in on-scene vehicles and among data terminal carried by users into buildings, etc.

Next Generation GETS and WPS address this.

Wireless Data

☑ Ability of on-scene personnel to transparently exchange, as authorized, text, image, and/or video data with other on-site personnel, dispatchers, data resources, etc.

Next Generation GETS and WPS address this.

Wireless Data

☑ Ability to protect the privacy of particular information according to applicable laws and statutes so that it can be accessed only by authorized personnel and data terminals.

Wireless Data

☑ Ability to ensure secure exchange of information.

For select users only.

Wireless Data

☑ Capability of high speed data transfer to allow fast exchange of text, image, and streaming video information.

In support of key user requirements.

Wireless Data

☑ Ability to remotely access a user's agency/jurisdiction data communications infrastructure when the user roams outside the radio coverage area of the user's agency/jurisdiction infrastructure.

Program/Organization:	**NCSBCS**
Full Name:	National Conference of States on Building Codes and Standards
Agencies:	
Partnering Agencies / Orgs.:	National Alliance for Building Regulatory Reform in the Digital Age; The Infrastructure Security Partnership (TISP); NIST; First Responders; Building Officials, State Emergency Managers
Web Page:	http://www.ncsbcs.org
Contact Name:	Robert C. Wible
	Executive Director
Contact Phone:	703-481-2035
Contact Email:	rwible@ncsbcs.org
Current Products:	o Website o Alliance and Teams to develop the project described below
Planned Products:	Proposed Secure, Interoperable, nationwide system of secure state-managed databases of building designs and evacuation plans for critical structures. The database will be 1. A multi-tiered "smart" database -- containing basic information on the nature of the hazard, more detailed information for incident commanders, yet more detailed information for incoming additional responders (especially if these come from other jurisdictions under mutual aid agreements); 2. Secure (encrypted with limited specific access) ; 3. Up-to-date (regarding construction information); 4. Current (with regard to potential and immediate hazards); 5. Capable of supporting searches; 6. Available 24/7 for contact information; 7. Connectable via online links to emergency, public safety information systems for additional levels of technical information relevant to safety of rescue personnel; 8. Linked and accessible by other jurisdictions; 9. Serviced by multiple software suppliers using secure, interoperable software; 10. Available through redundant systems--landlines and wireless, laptops and PDAs); 11. Coordinated with and linked to other first responder database information systems (e.g., emergency medical data, GIS systems).
Additional Information:	Additional contact: Carolyn Fitch, Program Coordinator at NCSBCS 703-481-2038
Program Goals:	Work with the Department of Homeland Security, FEMA, state and local homeland security directors, first responders, and governments, insurance, construction, and information technology communities to assemble interdisciplinary work team to do the following: o Define and set performance objectives of a coordinated state-based nationwide system to include: o Foster interactive hazard/incident-specific analysis capability o Assure data is transportable/interoperable and up to date o Assure data is secure.

Program/Organization:	NCSBCS			
Sectors Addressed:	☐ Law Enforcement	☐ Corrections	☑ EMS	☐ Military
	☐ Courts	☐ Probat./Parole	☑ Emerg. Manag.	☑ Other
	☐ Public Defender	☑ Fire Protection	☐ Transportation	Building Depts., Building Safety
	☐ Prosecution	☑ Public Works	☐ Utlities	

Functional Capabilities:

Wireless Voice

☑ Ability for users to transparently communicate, as authorized, with other members of the agency/jurisdiction on a unit-to-group (one-to-many) basis and a unit-to-unit (one-to-one) basis.

Wireless Voice

☑ Ability of the agency/jurisdiction to administer the priority for voice communications of particular users and particular applications (such as task force operations, incidents, etc.).

Wireless Voice

☑ Ability to have secure voice communications.

Wireless Voice

☑ Ability for users to transparently communicate, as authorized, among multiple agencies/jurisdictions some of which may use different technologies, infrastructures and/or frequency bands.

Wireless Voice

☑ Ability to remotely access a user's agency/jurisdiction voice communications infrastructure when the user roams outside the radio coverage area of the user's agency/jurisdiction wireless infrastructure.

Wireless Voice

☑ Ability to effectively initiate and sustain flexible and dynamic system administration (includes administration of talk groups, emergency alerts, networks, and channels for mutual aid).

Wireless Voice

☑ Ability to sustain highly reliable system performance across interconnected systems (including tolerance to individual system failures, redundant coverage from adjacent sites, resistance to impact of catastrophic events, etc).

Wireless Voice

☑ Ability to remotely (over-the-air) reprogram a user's radios and/or modify a user's encryption keys and/or modify a radio's waveforms. Maybe.

Wireless Voice

☑ Ability to provide state-wide (county-wide) signal coverage to vehicular/mobile radios on highways and at street level for state (county) agencies, to provide city-wide signal coverage to portable/handheld radios on the street and within buildings for city agencies, and to provide direct communications between user radios when there is no wireless infrastructure to support communications (such in some rural areas, underground parking garages, and inside some buildings).

Wireless Data

☑ Ability to initiate wireless data communications by requiring the user to only enter (on his/her data terminal/radio) a user identification which authenticates and validates the user, registers and sets data resource capabilities for the user, and completes all radio network administration for the user's data communications with other members of the user's agency/jurisdiction and with other agencies/jurisdictions, as authorized.

Wireless Data

☑ Ability of users to quickly and transparently establish on-scene wireless data networks that function among data terminals located in on-scene vehicles and among data terminal carried by users into buildings, etc.

Wireless Data

☑ Ability of on-scene personnel to transparently exchange, as authorized, text, image, and/or video data with other on-site personnel, dispatchers, data resources, etc.

Wireless Data

☑ Ability to protect the privacy of particular information according to applicable laws and statutes so that it can be accessed only by authorized personnel and data terminals.

Wireless Data

☑ Ability to ensure secure exchange of information.

Wireless Data

☑ Capability of high speed data transfer to allow fast exchange of text, image, and streaming video information.

Wireless Data

☑ Ability of transparent on-scene system access to multiple information systems regardless of differing data base system architectures and data formats.

Wireless Data

☑ Ability to remotely access a user's agency/jurisdiction data communications infrastructure when the user roams outside the radio coverage area of the user's agency/jurisdiction infrastructure.

Wireless Data

☑ Reliable system operational performance (including fault tolerant to individual system failures, redundant coverage from adjacent sites, full service during routine maintenance, and resistant to impact of catastrophic events).

Wireless Data

☑ Flexible and dynamic system administration (includes administration of on-scene wireless data networks).

Information Systems

☑ Ability to effectively and efficiently exchange data between agencies/jurisdictions, e.g., by employing common data representation structures and exchange formats and protocols.

Information Systems

☑ Ability to rapidly access subject information at critical decision points from both field and base locations, including but not limited to information regarding identification (photos, fingerprints, etc.) and activity (criminal history, wants/warrants, reporting/contact history, etc.).

Information Systems

☑ Ability to enter information once, then share and reuse that information among all entities that require it.

Information Systems

☑ Ability to query/access multiple data sources using one request that is routed to multiple entities simultaneously.

Information Systems

☑ Capability of standardized security, including functions and features that can be used to satisfy reasonable security requirements of any entity within a broader security framework.

Information Systems

☑ Ability to exchange information with Computer-Aided Dispatch (CAD) systems.

Information Systems

☑ Capability of field photo scanning and image file distribution.

Information Systems

☑ Ability to have near-real-time distribution of text messages to multiple organizations responding to a large event.

Information Systems

☑ Ability to access information related to hazardous materials, water sources, floor and building plans, utility maps, weather forecasts, topographic terrain, and other background data that may influence how public safety practitioners approach or conduct operations at an incident.

Information Systems

☑ Ability to access medical/treatment records (both those required to ensure proper treatment of incident victims and/or prisoners and those records obtained under warrant).

Information Systems

☑ Capability of automatic dissemination of disposition data to appropriate local, state, and federal agencies/databases.

Program/Organization:	**NDPIX**
Full Name:	National Drug Pointer Index (NDPIX)
Agencies:	U.S. Drug Enforcement Administration (DEA)
Partnering Agencies / Orgs.:	
Web Page:	http://www.usdoj.gov/dea/
Contact Name:	Mina Hunter
	Acting chief, NDPIX
Contact Phone:	(202) 307-3648
Contact Email:	mhunter@leo.gov
Current Products:	NDPIX, a Target Ceconfliction System: o Law enforcement agencies transmit to NDPIX identifying data on targets of active drug cases and the names and phone numbers of the investigating officers working these cases. NDPIX adds new entries to its database and matches the new entries to all earlier entries o For each computer detected match, NDPIX provides to both the entry maker and the record owner the name, agency and telephone number of the other o NDPIX operates on Department of Justice computers in Rockville, Maryland. Participating agencies communicate with NDPIX through the National Law Enforcement Telecommunications System (NLETS).
Planned Products:	National Virtual Pointer System (NVPS) DEA in partnership with the Regional Information Sharing System (RISS) and the High Intensity Drug Trafficking Areas (HIDTA) is developing NVPS to connect NDPIX, RISS, HIDTA and other target deconfliction systems. NVPS would cover all crimes.
Additional Information:	Judith Bertini, Deputy Assistant Administrator for Intelligence (202) 307-8748 jbertini@leo.gov
Program Goals:	

Sectors Addressed:	☑ ***Law Enforcement***	☐ ***Corrections***	☐ ***EMS***	☐ ***Military***
	☐ ***Courts***	☐ ***Probat./Parole***	☐ ***Emerg. Manag.***	☐ ***Other***
	☐ ***Public Defender***	☐ ***Fire Protection***	☐ ***Transportation***	
	☐ ***Prosecution***	☐ ***Public Works***	☐ ***Utlities***	

Program/Organization:	**NEMA**
Full Name:	National Emergency Management Association
Agencies:	National Association
Partnering Agencies / Orgs.:	o State emergency management directors o DHS o HHS (Office of Public Health Emergency Preparedness) o FEMA
Web Page:	http://www.nemaweb.org/index.cfm
Contact Name:	Kristin Robinson
	Government Relations Director
Contact Phone:	202-624-5460
Contact Email:	kcormier@csg.org
Current Products:	o Reports o Conferences and Summits for National Emergency Preparedness and Response Partners
Planned Products:	o Annual Conference and Exposition on Homeland Security and Emergency Management
Additional Information:	Each state has its own NEMA contact person.
Program Goals:	o to provide national leadership and expertise in comprehensive emergency management o to serve as a vital emergency management information and assistance resource o to advance continuous improvement in emergency management through strategic partnerships, innovative programs, and collaborative policy positions.

Sectors Addressed:	☐ ***Law Enforcement***	☐ ***Corrections***	☐ ***EMS***	☐ ***Military***
	☐ ***Courts***	☐ ***Probat./Parole***	☑ ***Emerg. Manag.***	☐ ***Other***
	☐ ***Public Defender***	☐ ***Fire Protection***	☐ ***Transportation***	
	☐ ***Prosecution***	☐ ***Public Works***	☐ ***Utlities***	

Program/Organization:	**NFPA**
Full Name:	National Fire Protection Association
Agencies:	IAB; Local, State, and Federal First Responders; Office of Domestic Preparedness (ODP); WHCA; EOP; CHICAGO EMCO; DoD HS ACTD; DCMPO
Partnering Agencies / Orgs.:	NFPA membership totals more than 75,000 individuals from around the world and more than 80 national trade and professional organizations
Web Page:	www.nfpa.org
Contact Name:	Stephen N. Foley
	Senior Fire Service Specialist, Public Fire Protection Division
Contact Phone:	617-984-7468
Contact Email:	sfoley@nfpa.org
Current Products:	NFPA develops, publishes, and disseminates timely consensus codes and standards intended to minimize the possibility and effects of fire and other risks. Virtually every building, process, service, design, and installation in society today is affected by NFPA documents. More than 300 NFPA codes and standards are used around the world. An example of a standard in progress is NFPA 1221 - "Standard for the Installation, Maintenance, and Use of Emergency Services Communications Systems."
Planned Products:	
Additional Information:	A report entitled, "A Needs Assessment of the U.S. Fire Service," FA-240/December 2002, was done by FEMA/USFA/NFPA and addressed communciations (among several other topics). The president of NFPA is James Shannon NFPA (National Fire Protection Association) 1 Batterymarch Park Quincy, MA 02169-7471 USA Telephone 617-770-3000
Program Goals:	The mission of the international nonprofit NFPA is to reduce the worldwide burden of fire and other hazards on the quality of life by providing and advocating scientifically based consensus codes and standards, research, training, and education.

Sectors Addressed:

☐ ***Law Enforcement***	☐ ***Corrections***	☐ ***EMS***	☐ ***Military***
☐ ***Courts***	☐ ***Probat./Parole***	☐ ***Emerg. Manag.***	☐ ***Other***
☐ ***Public Defender***	☑ ***Fire Protection***	☐ ***Transportation***	
☐ ***Prosecution***	☐ ***Public Works***	☐ ***Utlities***	

Program/Organization:	**NGA**
Full Name:	National Governors Association (Center for Best Practices)
Agencies:	National Association
Partnering Agencies / Orgs.:	Governors from the 50 states and Guam, Virgin Islands
Web Page:	http://www.nga.org
Contact Name:	Thom Rubel Program Director, State Information Technology Economic and Technology Policy Studies
Contact Phone:	202-624-7740
Contact Email:	trubel@nga.org
Current Products:	In March 2001, forty-two states were participating in NGA's Justice IT Integration Project, and were invited to submit proposals that would allow them to implement some piece of their strategic plans for statewide integrated justice. A panel of six reviewers representing NGA, the National Association of State Chief Information Officers, and the National Conference of State Courts recommended 26 states for awards. By the end of 2001, these 26 states were awarded a total of $16.4 million from the Bureau of Justice Assistance (BJA). On January 23-24, 2003, the NGA Center for Best Practices conducted a workshop for the 26 Justice Integration project states in Washington, DC. At the workshop, 21 of the 26 project states were in attendance to provide a status update on each of their projects and to receive assistance in furthering their project objectives through panel discussions by leading experts in the field of justice integration.
Planned Products:	
Additional Information:	Raymond C. Scheppach, Executive Director Joel Hirschorn 202/624-5346
Program Goals:	NGA provides governors and their senior staff members with services that range from representing states on Capitol Hill and before the Administration on key Federal issues to developing policy reports on innovative state programs and hosting networking seminars for state government executive branch officials. The NGA Center for Best Practices focuses on state innovations and best practices on issues that range from education and health to technology, welfare reform, and the environment. NGA also provides management and technical assistance to both new and incumbent governors.

Sectors Addressed:				
☐ ***Law Enforcement***	☐ ***Corrections***	☐ ***EMS***	☐ ***Military***
☑ ***Courts***	☐ ***Probat./Parole***	☐ ***Emerg. Manag.***	☐ ***Other***
☐ ***Public Defender***	☐ ***Fire Protection***	☐ ***Transportation***	
☐ ***Prosecution***	☐ ***Public Works***	☐ ***Utlities***	

Program/Organization:	**NIST**
Full Name:	National Institute of Standards and Technology
Agencies:	U.S. Department of Commerce
Partnering Agencies / Orgs.:	NIST, Project MESA, IEEE, IETF, and Public Safety communicators
Web Page:	www.nist.gov
Contact Name:	Nader Moayeri
	Manager, Wireless Communications Technologies Group
Contact Phone:	301-975-3767
Contact Email:	nader.moayeri@nist.gov

Current Products:	The NIST Distributed Testbed for First Responders: To evaluate different technical approaches and to carry out the NIST mission of assisting industry in the development of standards for interoperability and open systems, the National Institute of Standards and Technology (NIST) is developing a Distributed Testbed for First Responders. This testbed, which builds on work already underway in ITL, BFRL, and MEL, will enable collaborative research at NIST on issues relating to improving the safety and effectiveness of first responders. Research will be conducted on a variety of topics, including developing and demonstrating highly capable communication and localization systems, increasing the quality and quantity of information available to first responders, improving information display and decision support systems, and the use of smart wireless sensor networks in buildings.
Planned Products:	
Additional Information:	George E. Kelly Division 863 Chief BFRL ext. 5850
Program Goals:	The development of standards for highly capable first responder technologies that will incorporate the need for voice and data interoperability.

Sectors Addressed:

☑ *Law Enforcement*	☐ *Corrections*	☑ *EMS*	☐ *Military*
☐ *Courts*	☐ *Probat./Parole*	☑ *Emerg. Manag.*	☑ *Other*
☐ *Public Defender*	☑ *Fire Protection*	☐ *Transportation*	*Standards, Testing and Measurement*
☐ *Prosecution*	☐ *Public Works*	☐ *Utlities*	

Functional Capabilities:

Wireless Data

☑ Ability to initiate wireless data communications by requiring the user to only enter (on his/her data terminal/radio) a user identification which authenticates and

Using ad-hoc wireless networks to establish voice and data communications on-scene

validates the user, registers and sets data resource capabilities for the user, and completes all radio network administration for the user's data communications with other members of the user's agency/jurisdiction and with other agencies/jurisdictions, as authorized.

Wireless Data

☑ Ability of users to quickly and transparently establish on-scene wireless data networks that function among data terminals located in on-scene vehicles and among data terminal carried by users into buildings, etc.

Using ad-hoc wireless networks to establish voice and data communications on-scene

Wireless Data

☑ Ability of on-scene personnel to transparently exchange, as authorized, text, image, and/or video data with other on-site personnel, dispatchers, data resources, etc.

A NIST test-bed has been established to research, develop, and evaluate technologies that allow for voice/video/text/sensor data exchange capability. In addition, NIST's BFRL is working not only on organizing and sharing building data, but making it available in a graphical user interface that meets the needs of the first responder. Part of that display would be a floor plan of the building ("static" data). Along with this would be "dynamic" data such as location of fire activity, people, etc. BFRL will use the Virtual Cybernetic Building Testbed (VCBT) to simulate a fire and then format data from the VCBT in a display interface suitable for use by a first responder.

Wireless Data

☑ Capability of high speed data transfer to allow fast exchange of text, image, and streaming video information.

NIST has worked on these issues in the context of 3G wireless systems in the past. NIST is now developing the same capabilities in the context of wireless ad hoc networks, which are ideal for mission-critical operations.

Wireless Data

☑ Ability to remotely access a user's agency/jurisdiction data communications infrastructure when the user roams outside the radio coverage area of the user's agency/jurisdiction infrastructure.

The ad-hoc networks being developed at NIST have hooks to PSTN, to the Internet, and to the cellular networks.

Wireless Data

☑ Reliable system operational performance (including fault tolerant to individual system failures, redundant coverage from adjacent sites, full service during routine maintenance, and resistant to impact of catastrophic events).

The wireless ad hoc networks are being designed to degrade gracefully in face of such failures.

Wireless Data

☑ Flexible and dynamic system administration (includes administration of on-scene wireless data networks).

The wireless ad hoc networks being developed are working on self-organized networks, bypassing need for system administration.

Information Systems

☑ Ability to rapidly access subject information at critical decision points from both field and base locations, including but not limited to information regarding identification (photos, fingerprints, etc.) and activity (criminal history, wants/warrants, reporting/contact history, etc.).

NIST has developed a network architecture that provides communications at the scene of an emergency and is also connected to the Internet, to the PSTNs, etc.

Program/Organization:	**NIST**

Information Systems

☑ Ability to enter information once, then share and reuse that information among all entities that require it.	NIST is developing a publish/subscribe server for this purpose.

Information Systems

☑ Capability of field photo scanning and image file distribution.	The NIST Testbed has developed a prototype image transmission.

Information Systems

☑ Ability to have near-real-time distribution of text messages to multiple organizations responding to a large event.	The NIST Testbed is working with real-time audio/video streaming in addition to text messages, as well as multicasting.

Information Systems

☑ Ability to access information related to hazardous materials, water sources, floor and building plans, utility maps, weather forecasts, topographic terrain, and other background data that may influence how public safety practitioners approach or conduct operations at an incident.	NIST's BFRL is working not only on organizing and sharing building data, but making it available in a graphical user interface that meets the needs of the first responder. Part of that display would be a floor plan of the building ('static' data). Along with this would be 'dynamic' data such as location of fire activity, people, etc. BFRL will use the Virtual Cybernetic Building Testbed (VCBT) to simulate a fire and then format data from the VCBT in a display interface suitable for use by a first responder.

Information Systems

☑ Ability to access medical/treatment records (both those required to ensure proper treatment of incident victims and/or prisoners and those records obtained under warrant).	The Testbed has developed the capability to access such information through the Internet and other more secure means.

Information Systems

☑ Ability to access information regarding pending investigation/litigation of a particular subject.	The Testbed has developed the capability to access such information through the Internet and other more secure means.

Information Systems

☑ Ability to access court scheduling information.	The Testbed has developed the capability to access such information through the Internet and other more secure means.

Program/Organization:	NLECTC -- Southeast
Full Name:	National Law Enforcement and Corrections Technology Center
Agencies:	DoJ's National Institute of Justice
Partnering Agencies / Orgs.:	DoJ, NIJ/OST
Web Page:	http://www.nlectc.org
Contact Name:	Tommy Sexton
	Director
Contact Phone:	843-760-4626
Contact Email:	tsexton@nlectc-se.org

Current Products:	o Facilities across the country that are collocated with an organization or agency that specializes in one or more specific areas of research and development in law enforcement/corrections o A seamless web of support, providing (to law enforcement/corrections) technology assistance, support, and information o Quarterly newsletter, TechBeat and Law Enforcement & Corrections Technology (a news summary) o E-mail subscriptions o Training: Federal Law Enforcement Training Center Distance Learning o Videos: Technology on the Job, How We Can Talk, Surviving a Shooting: Your Guide to Personal Body Armor, OLETC 2000 Mock Prison Riot, Why Can't We Talk?, and Land Transportation Security Technology: An Improved Response for a Changing Threat o Equipment solutions o Excess Federal Property o Night Vision Devices o CTAC Technology Transfer Program o Public Safety Interoperable Communications Program (PSICP)
Planned Products:	--NLECTC-Southeast has conducted several Information Technology assessments in small, medium, and large law enforcement agencies, during which it became apparent that many agencies could benefit from a "roadmap" to implement information technology. Accordingly, the Center is developing the "Guidelines for Applying Information Technology in Law Enforcement." These Guidelines outline the use of business process re-engineering methodology to acquire information technology software and hardware. ---Software Adaptive Advanced Computing (SAAC) for Communications & Information Technology
Additional Information:	Created in 1994 as a component of the National Institute of Justice's (NIJ's) Office of Science and Technology, the National Law Enforcement and Corrections Technology Center (NLECTC) system serves as an "honest broker" offering support, research findings, and technological expertise to help state and local law enforcement and corrections personnel perform their duties more safely and efficiently. The NLECTC system is assisted in its work by national and regional advisory councils.

Because most of the country's law enforcement and corrections services are provided at the local level, the NLECTC system is composed of five regional centers and is complemented by several specialty offices and a national center. Most centers and offices are collocated with, or supported by, federally funded technology partners so they can leverage unique science and engineering expertise. The elements of the NLECTC System are presented below with contact material:

NLECTC-National
2277 Research Boulevard
Rockville, MD 20850
800-248-2742
asknlectc@nlectc.org

NLECTC-Northeast
26 Electronic Parkway
Rome, NY 13441-4514
888-338-0584
nlectc_ne@rl.af.mil

NLECTC-Southeast
5300 International Boulevard
North Charleston, SC 29418
800-292-4385
nlectc-se@nlectc-se.org

NLECTC-Rocky Mountain
2050 East Iliff Avenue
Denver, CO 80208
800-416-8086
nlectc@du.edu

NLECTC-West
c/o The Aerospace Corporation
2350 East El Segundo Boulevard
El Segundo, CA 90245-4691
888-548-1618
nlectc@law-west.org

NLECTC-Northwest
4000 Old Seward Highway, Suite 301
Anchorage, AK 99503-6068
866-569-2969
nlectc_nw@ctsc.net

Border Research and Technology Center (BRTC)
1010 Second Avenue, Suite 1920
San Diego, CA 92101-4912
888-656-2782
info@brtc.nlectc.org

Rural Law Enforcement Technology Center (RULETC)

Program/Organization:	**NLECTC -- Southeast**
	100 Bulldog Lane Hazard, KY 41701 866-787-2553 ruletc@aol.com Office of Law Enforcement Technology Commercialization (OLETC) 2001 Main Street, Suite 500 Wheeling, WV 26003 888-306-5382 oletc@oletc.org Office of Law Enforcement Standards (OLES) 100 Bureau Drive, Stop 8102 Gaithersburg, MD 20899-8102 301-975-2757 oles@nist.gov
Program Goals:	NLECTC-Southeast is collocated with its host, the South Carolina Research Authority in North Charleston, South Carolina. The Center's technology focus areas include information technology and technologies for corrections and school safety. NLECTC-Southeast helps law enforcement and corrections agencies acquire and redistribute Federal surplus/excess property. The Center also operates an Incident Mapping and Analysis Program that includes crime mapping training, spatial information management, geographic profiling, and data mining. The Center's technology partners include the Space and Naval Warfare Systems Center (SPAWAR)-Charleston, Oak Ridge National Laboratory, and Savannah River Technology Center.

Sectors Addressed:				
☑ *Law Enforcement*	☑ *Corrections*	☑ *EMS*	☑ *Military*
☐ *Courts*	☐ *Probat./Parole*	☑ *Emerg. Manag.*	☐ *Other*
☐ *Public Defender*	☑ *Fire Protection*	☐ *Transportation*	
☐ *Prosecution*	☐ *Public Works*	☐ *Utlities*	

Functional Capabilities:

Wireless Voice

☑ Ability to initiate wireless voice communications by requiring the user to only enter (on his/her radio) a user identification which authenticates and validates the user, registers and sets talk groups/capabilities for the user, and completes all radio network administration for the user's voice communications with other members of the user's agency/jurisdiction and with other agencies/jurisdictions, as authorized.	SAAC has shown the ability to 'autoaquire' FM handsets and automatically enter the handset into a call group.

Wireless Voice

☑ Ability for users to transparently communicate, as authorized, with other members of the agency/jurisdiction on a unit-to-group (one-to-many) basis and a unit-to-unit (one-to-one) basis.	The capability in the SAAC system allows both unit-to-group and unit-to-unit communications. In addition, this capability is provided over a large frequency space ranging from 20 MHz to 1.2 GHz

Wireless Voice	
☑ Ability of the agency/jurisdiction to administer the priority for voice communications of particular users and particular applications (such as task force operations, incidents, etc.).	The SAAC Team is working towards integrating the P 25 trunking standard, which supports the administration of priority access.
Wireless Voice	
☑ Ability to communicate an emergency voice message and/or signal which has priority over other voice communications.	The SAAC Team is working towards integrating the P 25 trunking standard, which supports emergency signaling.
Wireless Voice	
☑ Ability to have secure voice communications.	The SAAC system will incorporate the P 25 standard and will support the security called out in the P 25 specification.
Wireless Voice	
☑ Ability for users to transparently communicate, as authorized, among multiple agencies/jurisdictions some of which may use different technologies, infrastructures and/or frequency bands.	The crossbanding capability in the SAAC system has demonstrated the ability for multiple agencies to communicate over different frequencies.
Wireless Voice	
☑ Ability to sustain highly reliable system performance across interconnected systems (including tolerance to individual system failures, redundant coverage from adjacent sites, resistance to impact of catastrophic events, etc).	The design of the SAAC system uses multiple cards and only relies on the laptop for system configuration; the cards provide greater flexibility and redundancy in case of a single card or laptop failure.
Wireless Voice	
☑ Ability to remotely (over-the-air) reprogram a user's radios and/or modify a user's encryption keys and/or modify a radio's waveforms.	The SAAC Team is working towards integrating the P 25 trunking standard, which supports OTAR.
Wireless Voice	
☑ Ability to provide state-wide (county-wide) signal coverage to vehicular/mobile radios on highways and at street level for state (county) agencies, to provide city-wide signal coverage to portable/handheld radios on the street and within buildings for city agencies, and to provide direct communications between user radios when there is no wireless infrastructure to support communications (such in some rural areas, underground parking garages, and inside some buildings).	The SAAC system is deployable in a mobile configuration or can be collocated at a fixed tower location and can support requirements for multiple power levels.

Wireless Data

☑ Ability to initiate wireless data communications by requiring the user to only enter (on his/her data terminal/radio) a user identification which authenticates and validates the user, registers and sets data resource capabilities for the user, and completes all radio network administration for the user's data communications with other members of the user's agency/jurisdiction and with other agencies/jurisdictions, as authorized.

The SAAC Team is working towards integrating the P 25 trunking standard, which supports wireless data.

Wireless Data

☑ Ability of on-scene personnel to transparently exchange, as authorized, text, image, and/or video data with other on-site personnel, dispatchers, data resources, etc.

SAAC has demonstrated the ability to transfer jpg images over standard voice channels. This will be further enhanced for digital channels.

Wireless Data

☑ Ability to protect the privacy of particular information according to applicable laws and statutes so that it can be accessed only by authorized personnel and data terminals.

The SAAC system will use encryption and can support a secure data transmission requirement.

Wireless Data

☑ Ability to ensure secure exchange of information.

The SAAC system will use encryption and can support a secure data transmission requirement.

Wireless Data

☑ Capability of high speed data transfer to allow fast exchange of text, image, and streaming video information.

The SAAC system has been designed with a dynamic capability to widen the RF front end to provide a wideband capability for data transmission.

Information Systems

☑ Ability to effectively and efficiently exchange data between agencies/jurisdictions, e.g., by employing common data representation structures and exchange formats and protocols.

The SAAC Team is working towards integrating the P 25 trunking standard.

Information Systems

☑ Capability of field photo scanning and image file distribution.

The SAAC system is based on a standard PC-based architecture. Therefore any specific peripherals can be connected via USB ports for integration into the field. This could include scanners, fingerprint readers, etc.

Information Systems

☑ Ability to access information related to hazardous materials, water sources, floor and building plans, utility maps, weather forecasts, topographic terrain, and other background data that may influence how public safety practitioners approach or conduct operations at an incident.

SAAC is capable of Internet access and CD ROM access. Information available in these domains or other PC-compatible domains are accessible.

Information Systems

☑ Ability to access medical/treatment records (both those required to ensure proper treatment of incident victims and/or prisoners and those records obtained under warrant).

SAAC is capable of Internet access and CD ROM access. Information available in these domains or other PC-compatible domains are accessible.

Information Systems

☑ Ability to access information regarding pending investigation/litigation of a particular subject.	SAAC is capable of Internet access and CD ROM access. Information available in these domains or other PC-compatible domains are accessible.

Information Systems

☑ Ability to access court scheduling information.	SAAC is capable of Internet access and CD ROM access. Information available in these domains or other PC-compatible domains are accessible.

Program/Organization:	**NLETS**
Full Name:	National Law Enforcement Telecommunication System
Agencies:	State and Local Organization
Partnering Agencies / Orgs.:	1. Law enforcement workers 2. All 50 states and Canadian law enforcement
Web Page:	http://www.nlets.org/
Contact Name:	Fred Minice
	Director of Operations
Contact Phone:	602-224-0744
Contact Email:	fminice@nlets.org
Current Products:	1. A sophisticated, computer-controlled message switching network linking local, state, and federal agencies together to provide the capability to exchange criminal-justice and public-safety related information interstate 2. Frame-relay linking of state computers (403,000 LE & CJ terminals are able to send and receive un-secured messages using this NLETS) 3. Nationwide addressing scheme 4. The capability to exchange free-form criminal justice and criminal justice related information interstate. 5. The system is operated and controlled by the states. Every state is a member, while Federal systems such as the Federal Bureau of Investigation's National Crime Information Center (NCIC), U.S. Treasury's Treasury Enforcement Communications System (TECS), Department of Justice's System (JUST), Postal Inspection Service, Naval Investigation Service, Interpol, Air Force Office of Special Investigation, U.S. Secret Service, and the Department of State also utilize the network. 6. Interface with the Canadian Royal Mounted Police and the U.S. National Insurance Crime Bureau (NICB)
Planned Products:	
Additional Information:	Additional contact: Steve Correll 602-224-0744 scorrell@nlets.org
Program Goals:	o To provide within a secure environment, an international criminal-justice telecom capability that will benefit to the highest degree, the safety, security, and the preservation of human life and the protection of property o To assist those national and international governmental agencies and other organizations with similar missions who enforce or aid in enforcing local, state, Federal, or international laws or ordinances.

Sectors Addressed:				
☑ ***Law Enforcement***	☐ ***Corrections***	☑ ***EMS***	☑ ***Military***
☑ ***Courts***	☑ ***Probat./Parole***	☑ ***Emerg. Manag.***	☐ ***Other***
☑ ***Public Defender***	☑ ***Fire Protection***	☑ ***Transportation***	
☑ ***Prosecution***	☑ ***Public Works***	☐ ***Utlities***	

Program/Organization:	**NLETS**

Functional Capabilities:

Wireless Data

☑ Ability to initiate wireless data communications by requiring the user to only enter (on his/her data terminal/radio) a user identification which authenticates and validates the user, registers and sets data resource capabilities for the user, and completes all radio network administration for the user's data communications with other members of the user's agency/jurisdiction and with other agencies/jurisdictions, as authorized.	NLETS is offering this item by using multiple vendor partners who offer this service via the NLETS Frame Relay Network.

Wireless Data

☑ Ability of users to quickly and transparently establish on-scene wireless data networks that function among data terminals located in on-scene vehicles and among data terminal carried by users into buildings, etc.	NLETS is offering this item by using multiple vendor partners who offer this service via the NLETS Frame Relay Network.

Wireless Data

☑ Ability of on-scene personnel to transparently exchange, as authorized, text, image, and/or video data with other on-site personnel, dispatchers, data resources, etc.	NLETS is offering this item by using multiple vendor partners who offer this service via the NLETS Frame Relay Network.

Wireless Data

☑ Ability to protect the privacy of particular information according to applicable laws and statutes so that it can be accessed only by authorized personnel and data terminals.	NLETS is offering this item by using multiple vendor partners who offer this service via the NLETS Frame Relay Network.

Wireless Data

☑ Ability to ensure secure exchange of information.	NLETS is offering this item by using multiple vendor partners who offer this service via the NLETS Frame Relay Network.

Wireless Data

☑ Capability of high speed data transfer to allow fast exchange of text, image, and streaming video information.	NLETS is offering this item by using multiple vendor partners who offer this service via the NLETS Frame Relay Network.

Wireless Data

☑ Ability of transparent on-scene system access to multiple information systems regardless of differing data base system architectures and data formats.	NLETS is offering this item by using multiple vendor partners who offer this service via the NLETS Frame Relay Network.

Wireless Data

☑ Ability to remotely access a user's agency/jurisdiction data communications infrastructure when the user roams outside the radio coverage area of the user's agency/jurisdiction infrastructure.	NLETS is offering this item by using multiple vendor partners who offer this service via the NLETS Frame Relay Network.

Wireless Data

☑ Reliable system operational performance (including fault tolerant to individual system failures, redundant coverage from adjacent sites, full service during routine maintenance, and resistant to impact of catastrophic events).

NLETS is offering this item by using multiple vendor partners who offer this service via the NLETS Frame Relay Network.

Wireless Data

☑ Flexible and dynamic system administration (includes administration of on-scene wireless data networks).

NLETS is offering this item by using multiple vendor partners who offer this service via the NLETS Frame Relay Network.

Information Systems

☑ Ability to effectively and efficiently exchange data between agencies/jurisdictions, e.g., by employing common data representation structures and exchange formats and protocols.

Information Systems

☑ Ability to rapidly access subject information at critical decision points from both field and base locations, including but not limited to information regarding identification (photos, fingerprints, etc.) and activity (criminal history, wants/warrants, reporting/contact history, etc.).

Information Systems

☑ Ability to enter information once, then share and reuse that information among all entities that require it.

Information Systems

☑ Ability to query/access multiple data sources using one request that is routed to multiple entities simultaneously.

Information Systems

☑ Capability of standardized security, including functions and features that can be used to satisfy reasonable security requirements of any entity within a broader security framework.

Information Systems

☑ Ability to exchange information with Computer-Aided Dispatch (CAD) systems.

Information Systems

☑ Capability of field photo scanning and image file distribution.

Information Systems

☑ Ability to have near-real-time distribution of text messages to multiple organizations responding to a large event.

Program/Organization: **NLETS**

Information Systems

☑ Ability to access information related to hazardous materials, water sources, floor and building plans, utility maps, weather forecasts, topographic terrain, and other background data that may influence how public safety practitioners approach or conduct operations at an incident.

Information Systems

☑ Ability to access medical/treatment records (both those required to ensure proper treatment of incident victims and/or prisoners and those records obtained under warrant).

Information Systems

☑ Ability to access information regarding pending investigation/litigation of a particular subject.

Information Systems

☑ Ability to access court scheduling information.

Information Systems

☑ Ability to automatically link disposition data with charge data on subject RAP sheet/CCH information.

Information Systems

☑ Capability of automatic dissemination of disposition data to appropriate local, state, and federal agencies/databases.

Information Systems

☑ Ability to access current resource data (including personnel, equipment, materials, etc.) of multiple agencies/jurisdictions responding to a multi-agency/jurisdictional event by authorized users in the respective agencies/jurisdictions.

Program/Organization:	**NPSTC**
Full Name:	National Public Safety Telecommunications Council
Agencies:	Federation of associations representing Public Safety telecommunications
Partnering Agencies / Orgs.:	o International Municipal Signal Association (IMSA) o International Association of Emergency Managers (IAEM) o Forestry Conservation Communications Association (FCCA) o National Association of State Telecommunications Directors (NASTD) o International Association of Chiefs of Police (IACP) o American Association of State Highway Transportation Officials (AASHTO) o International Association of Fire Chiefs (IAFC) o Association of Public-Safety Communications Officials--International (APCO) o International Association of Fish and Wildlife Agencies (IAFWA) o National Association of State Emergency Medical Services Directors (NASEMSD) o National Association of State Foresters (NASF) o American Radio Relay League (ARRL) o American Red Cross (ARC)
Web Page:	http://www.npstc.org
Contact Name:	Marilyn Ward
	Chair, NPSTC
Contact Phone:	407-836-9668
Contact Email:	Marilyn.Ward@ocfl.net
Current Products:	o 700 MHz Pre-coordination Database o User requirements/specifications for Project MESA o Regional planning support o National Coordination Committee (NCC) support o ITU-R Working Party 8A support o 800 MHz Public Safety interference resolution o U.S./Canadian DTV transition issues
Planned Products:	o User requirements for software defined radio (SDR) and participation on SDR Forum o User requirements for wideband data services in 4.9 GHz band
Additional Information:	Steve Devine 573-526-6105 devins@mshp.state.mo.us
Program Goals:	o To develop and make recommendations regarding Public Safety communications issues and policies that promote interoperability and cooperation between Federal, state, and local agencies o To serve as a standing forum for the exchange of ideas and information o To identify and promote methods for funding development of Public Safety communications systems o To conduct studies of Public Safety communications and use research to stay abreast of user needs

Sectors Addressed:	☑ ***Law Enforcement***	☐ ***Corrections***	☑ ***EMS***	☐ ***Military***
	☐ ***Courts***	☐ ***Probat./Parole***	☑ ***Emerg. Manag.***	☑ ***Other***

Program/Organization:	**NPSTC**

☐ *Public Defender*	☑ *Fire Protection*	☑ *Transportation*	*Forestry, Fish and Wildlife*
☐ *Prosecution*	☐ *Public Works*	☐ *Utlities*	

Functional Capabilities:

Wireless Voice

☑ Ability to provide state-wide (county-wide) signal coverage to vehicular/mobile radios on highways and at street level for state (county) agencies, to provide city-wide signal coverage to portable/handheld radios on the street and within buildings for city agencies, and to provide direct communications between user radios when there is no wireless infrastructure to support communications (such in some rural areas, underground parking garages, and inside some buildings).	The Missouri State Highway Patrol operates a low VHF band (42 MHz) statewide radio system that has complete coverage over the entire state of Missouri from 15 sites. We anticipate eventually moving to a higher band and using some of the trunking functionality that is mentioned above, but the time frame for that transition is undecided.

Wireless Data

☑ Ability to initiate wireless data communications by requiring the user to only enter (on his/her data terminal/radio) a user identification which authenticates and validates the user, registers and sets data resource capabilities for the user, and completes all radio network administration for the user's data communications with other members of the user's agency/jurisdiction and with other agencies/jurisdictions, as authorized.	The Missouri State Highway Patrol uses commercial Cellular Digital Packet Data throughout most of the state.

Information Systems

☑ Ability to exchange information with Computer-Aided Dispatch (CAD) systems.	Via the above-mentioned CDPD network, the CDPD allows mobile units statewide to access the statewide MSHP CAD Dispatch system.

Program/Organization:	**NRL / InfraLynx**
Full Name:	Naval Research Laboratory / InfraLynx
Agencies:	Dept. of Navy; Naval Research Lab (NRL); Dept. of Defense
Partnering Agencies / Orgs.:	IAB; local, state, and Federal First Responders; Office of Domestic Preparedness (ODP); WHCA; EOP; Chicago EMCO; DoD HS ACTD; DCMPD
Web Page:	InfraLynx.nrl.navy.mil or NRL.NAVY.MIL
Contact Name:	Chris Herndon / Dave DeRieux
Contact Phone:	202-767-6525 202-767-0002
Contact Email:	herndon@ttdl.nrl.navy.mil/ derieux@kingcrab.nrl.mil
Current Products:	InfraLynx scalable communications are available in many configurations/vehicles. InfraLynx is a rapidly deployable, interoperable communications infrastructure that provides high assurance telephony, network, and radio connectivity.
Planned Products:	InfraLynx communications enhancements; wireless integration; wireless voice and data communications
Additional Information:	NRL provides technology and communications support to ODP / PEP as requested under an interagency agreement (IAA) with ODP. InfraLynx provides immediate response telephony and data/network services either as a stand-alone system or as an augmentation to existing or emerging C3 systems. InfraLynx's universal command and control toolkit uses common components to minimize training, and eliminates duplicative, non-interoperable, proprietary solutions to improve long-term supportability. - phone service (POTS, STU, and FAX) - private cellular network - conventional communications (HF/VHF/UHF/800) - VOIP connectivituy (VTC, communications) - communications crossband and gateway - networks (VPN, NIPR, SIPRNET) - video uplink/downlink via satellite (KA/KU SATCOM)
Program Goals:	1. Provide a broad range of interoperable communications support for first responders with reach-back and reconstituion capabilities. 2. Support the weapons of mass destruction (WMD) prepositioned equipment program (PEP), which provides specially selected equipment prepositioned to aid local and state emergency response authorities whose jurisdictions become the target of WMD terrorism. The PEP program's primary goal is to deliver, in a timely manner, equipment to a designated incident command logistics site anywhere in the United States.

Sectors Addressed:				
	☐ ***Law Enforcement***	☐ ***Corrections***	☐ ***EMS***	☐ ***Military***
	☐ ***Courts***	☐ ***Probat./Parole***	☐ ***Emerg. Manag.***	☐ ***Other***
	☐ ***Public Defender***	☐ ***Fire Protection***	☐ ***Transportation***	
	☐ ***Prosecution***	☐ ***Public Works***	☐ ***Utlities***	

Program/Organization:	**NRL / InfraLynx**

Functional Capabilities:

Wireless Voice

☑ Ability to initiate wireless voice communications by requiring the user to only enter (on his/her radio) a user identification which authenticates and validates the user, registers and sets talk groups/capabilities for the user, and completes all radio network administration for the user's voice communications with other members of the user's agency/jurisdiction and with other agencies/jurisdictions, as authorized.	The NRL I nfraLynx provides a host of off-the-shelf integrated communications gear. One important element is the ACU 1000 along with the associated radios compromising the first responder incident spectrum.

Wireless Voice

☑ Ability for users to transparently communicate, as authorized, with other members of the agency/jurisdiction on a unit-to-group (one-to-many) basis and a unit-to-unit (one-to-one) basis.	The NRL InfraLynx provides a host of off-the-shelf integrated communications gear. The "one-to-many" and "unit-to-unit" communications is handled via the ACU-1000 and/or the TAC-CELL cellular switch and/or a satellite data modem and/or wireless voice /data/video (802.11a/b)

Wireless Voice

☑ Ability of the agency/jurisdiction to administer the priority for voice communications of particular users and particular applications (such as task force operations, incidents, etc.).	The InfraLynx system can coordinate priority voice and data communications via an existing off-the-shelf suite of radios tailored for the incident. The InfraLynx can also pass the GETS card information. In the future, the development of a Software Definable Radio (SDR) will be able to seamlessly accomplish the task. The NRL has developed an SDR "Pathfinder" and demonstrated this capability in conjunction with the InfraLynx in 2002 at O'Hare International Airport in Chicago. Additionally, the Satellite and cellular systems can also be prioritized based on task force operations guidance.

Wireless Voice

☑ Ability to communicate an emergency voice message and/or signal which has priority over other voice communications.	The InfraLynx system provides existing radio types to facilitate emergency broadcast. In addition, the InfraLynx can be programmed to use satellite and cellular system for a priority voice.

Wireless Voice

☑ Ability to have secure voice communications.	The InfraLynx system provides off-the-shelf radio types that facilitate secure voice communications. In addition, InfraLynx utilizes the secure type 3 encryption for cell phones via Verizon.

Wireless Voice

☑ Ability for users to transparently communicate, as authorized, among multiple agencies/jurisdictions some of which may use different technologies, infrastructures and/or frequency bands.	The InfraLynx achieves this interoperability among disparate users by providing each radio type as well as utilizing the ACU 1000. In addition, the internet is also used a point of presence for all agencies to log on to. In the future, the SDR will be programmed to facilitate interagency communications.

Wireless Voice

☑ Ability to remotely access a user's agency/jurisdiction voice communications infrastructure when the user roams outside the radio coverage area of the user's agency/jurisdiction wireless infrastructure.	The InfraLynx provides a complete communications extension. Once on scene, the user can access all existing radios, internet, cell and satellite services to restore local communications and provide a reach back capability.

Program/Organization:	**NRL / InfraLynx**

Wireless Voice

☑ Ability to effectively initiate and sustain flexible and dynamic system administration (includes administration of talk groups, emergency alerts, networks, and channels for mutual aid).

The InfraLynx system provides the ACU 1000 for radio programming. The resident TAC-CELL can be programmed for talk groups, emergency alerts and mutual aid. The satellite system can be programmed by the system administrator in a primary or back mode. InfraLynx uses a series of advanced network monitoring tools for wireless and wired communications..

Wireless Voice

☑ Ability to sustain highly reliable system performance across interconnected systems (including tolerance to individual system failures, redundant coverage from adjacent sites, resistance to impact of catastrophic events, etc).

The InfraLynx system provides a highly reliable redundant multifaceted communication suite comprised of multiple radios, satellite system and cellular switch and WIFI. In the event of a catastrophe, these systems can be used individually or as group (scaleable, depending on mission parameters).

Wireless Voice

☑ Ability to remotely (over-the-air) reprogram a user's radios and/or modify a user's encryption keys and/or modify a radio's waveforms.

The InfraLynx provides off-the-shelf commercial communications equipment and thus could employ those components that would enable over-the-air rekey, modification of encryptions keys and modification of radio waveforms.

Wireless Voice

☑ Ability to provide state-wide (county-wide) signal coverage to vehicular/mobile radios on highways and at street level for state (county) agencies, to provide city-wide signal coverage to portable/handheld radios on the street and within buildings for city agencies, and to provide direct communications between user radios when there is no wireless infrastructure to support communications (such in some rural areas, underground parking garages, and inside some buildings).

The InfraLynx provides a self contained, complete complement of communications gear including radios corresponding to jurisdictional requirements. In addition, the ACU 1000 enables the crossbanding between radios. Once a signal reaches the InfraLynx, it can be routed via radio, cellular, WIFI and/or satcom. In circumstances where there is no infrastructure, InfraLynx can provide the bridge to the outside world. InfraLynx is the contingency.

Wireless Data

☑ Ability to initiate wireless data communications by requiring the user to only enter (on his/her data terminal/radio) a user identification which authenticates and validates the user, registers and sets data resource capabilities for the user, and completes all radio network administration for the user's data communications with other members of the user's agency/jurisdiction and with other agencies/jurisdictions, as authorized.

The InfraLynx system uses the Windows 2000 authentication server as well as, WEP, AES encryption and MAC address for authentication and validation.

Wireless Data

☑ Ability of users to quickly and transparently establish on-scene wireless data networks that function among data terminals located in on-scene vehicles and among data terminal carried by users into buildings, etc.

The InfraLynx functions as a local wireless provider by providing the conduit to reach the first responder in vehicles, buildings, field and in remote locations.

Wireless Data

☑ Ability of on-scene personnel to transparently exchange, as authorized, text, image, and/or video data with other on-site personnel, dispatchers, data resources, etc.

The InfraLynx provides software collaborative tools such as Net Meeting and CMI services.

Program/Organization:	**NRL / InfraLynx**

Wireless Data

☑ Ability to protect the privacy of particular information according to applicable laws and statutes so that it can be accessed only by authorized personnel and data terminals.	InfraLynx provides several levels of security, such as 3 DES, AES and WEB standards.

Wireless Data

☑ Ability to ensure secure exchange of information.	InfraLynx provides several levels of security, such as 3 DES, AES and WEB standards

Wireless Data

☑ Capability of high speed data transfer to allow fast exchange of text, image, and streaming video information.	InfraLynx can deliver up a maximum 20 Mbps of thru put

Wireless Data

☑ Ability of transparent on-scene system access to multiple information systems regardless of differing data base system architectures and data formats.	The InfraLynx acts as a conduit for data to different systems and architecture. The InfraLynx follows Layer 3 of the OSI stack

Wireless Data

☑ Ability to remotely access a user's agency/jurisdiction data communications infrastructure when the user roams outside the radio coverage area of the user's agency/jurisdiction infrastructure.	The InfraLynx is an extension of the local infrastructure. The use of satcom technology enables the first responder to reach back in remote areas OR areas of devastated communications.

Wireless Data

☑ Reliable system operational performance (including fault tolerant to individual system failures, redundant coverage from adjacent sites, full service during routine maintenance, and resistant to impact of catastrophic events).	The InfraLynx was designed to be a communication infrastructure reconstruction tool. InfraLynx is the contingency.

Wireless Data

☑ Flexible and dynamic system administration (includes administration of on-scene wireless data networks).	The InfraLynx system provides numerous off-the-shelf wireless devices, a cell switch and satcom data modem. All are designed to work seamlessly with existing first responder wireless gear or can be programmed for talk groups, emergency alerts and mutual aid. The satellite system can be programmed by the system administrator in a primary or back mode. InfraLynx uses a series of advanced network monitoring tools for wireless and wired communications.

Information Systems

☑ Ability to effectively and efficiently exchange data between agencies/jurisdictions, e.g., by employing common data representation structures and exchange formats and protocols.	The InfraLynx is the conduit, providing the collection and dissemination of data to effectively enable existing first responder information systems to perform as designed

Program/Organization:	**NSA**
Full Name:	National Sheriffs' Association
Agencies:	National Association
Partnering Agencies / Orgs.:	o Sheriffs, deputies, law enforcement/public safety professionals, and concerned citizens o Funding (Federal Grants) comes from the U.S. DoJ, OJP, Office for Victims of Crime (OVC) and from BJA
Web Page:	http://www.sheriffs.org/contactus/index.htm
Contact Name:	Harlin McEwen Communications Advisor
Contact Phone:	607-275-1522
Contact Email:	ChiefHRM@leo.gov
Current Products:	
Planned Products:	
Additional Information:	National Sheriffs' Association 1450 Duke Street Alexandria, VA 22314-3490 703/836-7827 nsamail@sheriffs.org Training: jwright@sheriffs.org Director of Training and Manager of the Grant Project re: Interoperability: Mr. Fred Wilson 703/838-5322 Global contact: Mr. John Thompson 703/836-5313
Program Goals:	o To collect and share information to assist law enforcement officials in cooperative networking and in carrying out their duties efficiently o To conduct such research, study, and investigation as may be necessary and advisable to develop information, knowledge, and data which would be useful in improving the administration of criminal justice o With training, to promote the law enforcement profession by providing appropriate educational courses in cooperation with institutions of higher learning o To conduct competitions and make awards for outstanding services to all areas of the criminal justice community

Sectors Addressed:				
☑ ***Law Enforcement***	☑ ***Corrections***	☐ ***EMS***	☐ ***Military***
☐ ***Courts***	☐ ***Probat./Parole***	☐ ***Emerg. Manag.***	☐ ***Other***
☐ ***Public Defender***	☐ ***Fire Protection***	☐ ***Transportation***	
☐ ***Prosecution***	☐ ***Public Works***	☐ ***Utlities***	

Program/Organization:	**NTIA Public Safety Program 6/30/03**
Full Name:	National Telecommunications and Information Administration Public Safety Program
Agencies:	U.S. Department of Commerce, NTIA/Office of Spectrum Management
Partnering Agencies / Orgs.:	
Web Page:	http://ntiacsd.ntia.doc.gov/pubsafe/
Contact Name:	Don Speights
	Program Manager
Contact Phone:	202-482-4276
Contact Email:	wspeights@ntia.doc.gov

Current Products:

Primary Products
- Spectrum Regulatory Rules and Regulations
- Spectrum Management Policy
- Executive Branch Spectrum Management Initiative
- Partnerships and Consultation
  - o PSWN Executive Committee
  - o APCO
  - o NCC
  - o Partnership for Public Warning
  - o All Hazards Inter-Agency WG
- Technology standards
  - o P25
  - o Project MESA
  - o IO Technology Policy
- Spectrum efficiency
- Spectrum sharing initiatives and joint systems development
- Federal Wireless Users Forum Chair
- Recent Reports and Current Studies
  - o Current and Future Spectrum Use by the Energy, Water, and Railroad Industries
  - o Alternative Frequencies for use by Public Safety Systems
  - o Spectrum Efficiency Initiative
  - o Interoperable Technology Study

- International Assistance
  - o Joint Communications Board Iraq
  - o USTTI Spectrum Management Training
  - o WRC Public Safety issue support WP8

Planned Products:

Additional Information:

Program/Organization:	**NTIA Public Safety Program 6/30/03**
Program Goals:	o To coordinate the various spectrum related public safety programs within the Federal Government and to formulate Administration telecom policy dealing with Federal, State, and local public safety telecommunications.

Sectors Addressed:				
☑ *Law Enforcement*	☐ *Corrections*	☐ *EMS*	☑ *Military*
☐ *Courts*	☐ *Probat./Parole*	☑ *Emerg. Manag.*	☐ *Other*
☐ *Public Defender*	☑ *Fire Protection*	☐ *Transportation*	
☐ *Prosecution*	☐ *Public Works*	☐ *Utlities*	

Program/Organization:	**OASIS**
Full Name:	Organization for the Advancement of Structured Information Standards
Agencies:	
Partnering Agencies / Orgs.:	
Web Page:	http://www.oasis-open.org/who/
Contact Name:	Karl F. Best
	Director, Technical Operations
Contact Phone:	978-667-5115
Contact Email:	karl.best@oasis-open.org
Current Products:	1. OASIS operates XML.org, a community clearinghouse for XML application schemas, vocabularies, and related documents. 2. OASIS hosts the Cover Page, an online reference collection for interoperable markup language standards. 3. OASIS produces worldwide standards for security, Web services, XML conformance, business transactions, electronic publishing, topic maps, and interoperability within and between marketplaces.
Planned Products:	
Additional Information:	
Program Goals:	o to develop, promote, and foster convergence and adoption of e-business standards.

Sectors Addressed:	☑ *Law Enforcement*	☑ *Corrections*	☑ *EMS*	☑ *Military*
	☑ *Courts*	☑ *Probat./Parole*	☑ *Emerg. Manag.*	☐ *Other*
	☑ *Public Defender*	☑ *Fire Protection*	☑ *Transportation*	
	☑ *Prosecution*	☑ *Public Works*	☑ *Utlities*	

Program/Organization:	**ODP**
Full Name:	Office of Domestic Preparedness
Agencies:	Department of Homeland Security, Border & Transportation Directorate
Partnering Agencies / Orgs.:	
Web Page:	www.ojp.usdoj.gov/odp
Contact Name:	Frank LePage
Contact Phone:	202-305-9887
Contact Email:	lepage@ojp.usdoj.gov

Current Products:	o Emergency Responder Guidelines o HDER (Homeland Defense Equipment Reuse) Program o DPETAP (Domestic Preparedness Equipment Technical Assistance Program) in ODP o Application kit for the Domestic Preparedness Grant Application Program o Six national training centers under the National Domestic Preparedness Consortium (also in the OPD WMD Training Program) o An On-Line Data Collection Tool
Planned Products:	o Six national training centers under the National Domestic Preparedness Consortium (also in the OPD WMD Training Program) o An On-Line Data Collection Tool
Additional Information:	Frank LePage, general number: 202/305-9887 press number: 202/514-2000 www.ojp.usdoj.gov/odp 1-800-368-6498 ODP State & Local Domestic Preparedness Support Helpline: 1-800-368-6498 www.ojp.usdoj.gov/odp/ Grants hotline: http://www.grantshotline.com/phsfh/index.shtml
Program Goals:	o Training to enhance the capabilities of state and local first responders to deal with the threat of domestic terrorism involving weapons of mass destruction (WMD) o Funding for tools and equipment to assist state and local first responders in responding to acts of terrorism and related emergencies o Assisting in needs assessment and access to emergency data

Sectors Addressed:	☑ ***Law Enforcement***	☐ ***Corrections***	☑ ***EMS***	☐ ***Military***
	☐ ***Courts***	☐ ***Probat./Parole***	☑ ***Emerg. Manag.***	☐ ***Other***
	☐ ***Public Defender***	☑ ***Fire Protection***	☑ ***Transportation***	
	☐ ***Prosecution***	☑ ***Public Works***	☐ ***Utlities***	

Program/Organization:	**ODP**

Functional Capabilities:

Wireless Voice

☑ Ability for users to transparently communicate, as authorized, among multiple agencies/jurisdictions some of which may use different technologies, infrastructures and/or frequency bands.

The Office for Domestic Preparedness (ODP) is providing training and technical assistance to enhance interoperable communications in state and local agencies. Although this effort is ramping up, it will be available soon to a limited number of local jurisdictions and selected state agencies, particularly large cities funded through the ODP Urban Area Security Initiative (UASI). State agencies also will be eligible for this assistance. State and local agencies, with ODP assistance will be able to conduct requirements analyses and assessments, develop engineering recommendations to improve communications interoperability, and learn how to utilize work around technologies; i.e., cross-band switching devices, in the solution process. This builds on the work ODP has already accomplished under a FY 1999 interoperable communications demonstration project. The demo project placed 52 ACU/TRP-1000 cross switches in 22 jurisdictions which also included on-site training, evaluation, and the development of an ACU/TRP-1000 users guide for jurisdictional use. Several of the jurisdictions that had received these devices are also UASI cities and will be slated for additional assistance in interoperable communications.

Wireless Data

☑ Ability of users to quickly and transparently establish on-scene wireless data networks that function among data terminals located in on-scene vehicles and among data terminal carried by users into buildings, etc.

The OPD provides funding in the amount of $20 million for CAPWIN, the Capitol Area Wireless Integration Network, a project designed to demonstrate, test, and evaluate a web based information tool, used by patrol officers, hazardous materials transporters, and emergency management officials. CAPWIN users are able to obtain real-time information on suspect individuals, hazardous cargo, and terrorist activities involving weapons of mass destruction. ODP funding for this project provides resources to design and develop the information architecture using non-proprietary software, a systems integration team, State and local agency participants to conduct field tests and evaluations for this capability. The ODP is working in partnership with the National Institute of Justice (NIJ) as co-managers of CAPWIN. It is anticipated that future funding in FY 2004 is forthcoming to continue to build upon the successes of CAPWIN and expand the number of project sites. Although CAPWIN is a data only capability, an additional requirement to establish voice communications capabilities is anticipated.

Program/Organization:	**OLES**
Full Name:	Office of Law Enforcement Standards
Agencies:	U.S. DoC, National Institute of Standards and Technology
Partnering Agencies / Orgs.:	National Institute of Justice AGILE Program DHS Science and Technology Directorate SAFECOM Office of Domestic Preparedness
Web Page:	http://www.eeel.nist.gov/oles/
Contact Name:	Kathleen Higgins
	Director, NIST/OLES
Contact Phone:	301-975-2757
Contact Email:	kathleen.higgins@nist.gov
Current Products:	On behalf of NIJ's AGILE Program: o Successfully coordinated with OJP and BJA to advance standardization objectives of the Global Justice information sharing initiative (GLOBAL) and its Advisory Committee (a Presidential Advisory body) o Provided technical support to GLOBAL's Infrastructure/Standards Working Group (I/SWG) by: (1) developing I/SWG processes and procedures outlining salient technical issues to address relative to information sharing and (2) working with practitioners to create effective standardized solutions o Worked closely with diverse members of the Justice community to reconcile several different implementation standards applying XML (eXtensible Markup Language) and to develop a "Justice XML Data Dictionary" that contains over 2000 data elements that can be used commonly across the Justice community o Coordinated with Department of Transportation and other "Justice Partners" to share Justice work results and establish common interoperability schemes
Planned Products:	
Additional Information:	
Program Goals:	The mission of OLES is to serve as the principal agent for standards development for the criminal justice and public safety communities. OLES has been instrumental in the development of numerous standards and the issuance of various technical reports that have had significant impact on both of these communities. OLES helps criminal justice and public safety agencies acquire, on a cost-effective basis, the high quality resources they need to do their jobs. To accomplish this task, OLES: o Develops methods for testing equipment performance; o Develops methods for examining evidentiary materials; o Develops standards for equipment and operating procedures; o Develops users' guides; o Develops standard reference materials; and o Performs other scientific and engineering research as required by the criminal justice and public safety communities.

Program/Organization:	OLES			
Sectors Addressed:	☑ Law Enforcement	☑ Corrections	☑ EMS	☐ Military
	☑ Courts	☑ Probat./Parole	☑ Emerg. Manag.	☐ Other
	☑ Public Defender	☑ Fire Protection	☑ Transportation	
	☑ Prosecution	☐ Public Works	☐ Utlities	

Functional Capabilities:

Wireless Voice

☑ Ability to initiate wireless voice communications by requiring the user to only enter (on his/her radio) a user identification which authenticates and validates the user, registers and sets talk groups/capabilities for the user, and completes all radio network administration for the user's voice communications with other members of the user's agency/jurisdiction and with other agencies/jurisdictions, as authorized.	On behalf of the NIJ AGILE Program and COPS, standards development in Project 25, Project MESA, NPSTC working groups, and the Software Defined Radio Forum; and acquisition, test and evaluation of Project 25 equipment and interoperability devices.

Wireless Voice

☑ Ability for users to transparently communicate, as authorized, with other members of the agency/jurisdiction on a unit-to-group (one-to-many) basis and a unit-to-unit (one-to-one) basis.	On behalf of the NIJ AGILE Program and COPS, standards development in Project 25, Project MESA, NPSTC working groups, and the Software Defined Radio Forum; and acquisition, test and evaluation of Project 25 equipment and interoperability devices.

Wireless Voice

☑ Ability of the agency/jurisdiction to administer the priority for voice communications of particular users and particular applications (such as task force operations, incidents, etc.).	On behalf of the NIJ AGILE Program and COPS, standards development in Project 25, and Project MESA

Wireless Voice

☑ Ability to communicate an emergency voice message and/or signal which has priority over other voice communications.	On behalf of the NIJ AGILE Program, standards development in Project 25, and Project MESA especially in areas related to quality of service and priority access parameters.

Wireless Voice

☑ Ability to have secure voice communications.	On behalf of the AGILE Program, standardization through direct technical support to Project 25, Project MESA, NPSTC working groups, and the Software Defined Radio Forum), test and evaluation of prospective standardized approaches (before they are offered to standards committees), and test and evaluation of standard products to determine the degree of interoperability among them.

Wireless Voice

☑ Ability for users to transparently communicate, as authorized, among multiple agencies/jurisdictions some of which may use different technologies, infrastructures and/or frequency bands.	On behalf of the NIJ AGILE Program and COPS, standards development in Project 25, Project MESA, NPSTC working groups, and the Software Defined Radio Forum; and acquisition, test and evaluation of Project 25 equipment and commercially available and emerging interoperability devices.

Program/Organization:	**OLES**

Wireless Voice

☑ Ability to remotely access a user's agency/jurisdiction voice communications infrastructure when the user roams outside the radio coverage area of the user's agency/jurisdiction wireless infrastructure.	On behalf of NIJ's AGILE Program and COPS, development of specifications for Standards in Project 25, Project MESA, NPSTC working groups, and the Software Defined Radio Forum), test and evaluation of prospective standardized approaches (before they are offered to standards committees), acquisition and test and evaluation of standard products to determine the degree of interoperability among them, and test and evaluation of commercially available and emerging interoperability devices.

Wireless Voice

☑ Ability to effectively initiate and sustain flexible and dynamic system administration (includes administration of talk groups, emergency alerts, networks, and channels for mutual aid).	On behalf of NIJ's AGILE Program, standardization through direct technical support to Project 25, Project MESA, NPSTC working groups, and the Software Defined Radio Forum), test and evaluation of prospective standardized approaches (before they are offered to standards committees), and test and evaluation of standard products to determine the degree of interoperability among them.

Wireless Voice

☑ Ability to sustain highly reliable system performance across interconnected systems (including tolerance to individual system failures, redundant coverage from adjacent sites, resistance to impact of catastrophic events, etc).	On behalf of NIJ's AGILE Program and COPS, wireless research and standardization of performance in adverse environments in conjunction with Project 25, Project MESA, NPSTC working groups, and the Software Defined Radio Forum. Also, test and evaluation of prospective standardized approaches (before they are offered to standards committees), and test and evaluation of standard products to determine the degree of interoperability among them.

Wireless Voice

☑ Ability to remotely (over-the-air) reprogram a user's radios and/or modify a user's encryption keys and/or modify a radio's waveforms.	On behalf of NIJ's AGILE Program, efforts associated with standardization (through direct technical support to Project 25, Project MESA, NPSTC working groups, and the Software Defined Radio Forum), test and evaluation of prospective standardized approaches (before they are offered to standards committees), and test and evaluation of standard products to determine the degree of interoperability among them.

Wireless Voice

☑ Ability to provide state-wide (county-wide) signal coverage to vehicular/mobile radios on highways and at street level for state (county) agencies, to provide city-wide signal coverage to portable/handheld radios on the street and within buildings for city agencies, and to provide direct communications between user radios when there is no wireless infrastructure to support communications (such in some rural areas, underground parking garages, and inside some buildings).	On behalf of NIJ's AGILE Program and COPS, research, analysis and development efforts related to the propagation of wireless communications signals in urban environments, and evaluation of system alternatives. Also, related standards development efforts (including laboratory evaluation work) associated with Project 25, Project MESA, NPSTC working groups, and the Software Defined Radio Forum). And test and evaluation of commercially available and emerging interoperability devices.

Wireless Data

☑ Ability to initiate wireless data communications by requiring the user to only enter (on his/her data terminal/radio) a user identification which authenticates and validates the user, registers and sets data resource capabilities for the user, and completes all radio network administration for the user's data communications with other members of the user's agency/jurisdiction and with other agencies/jurisdictions, as authorized.	On behalf of the NIJ AGILE Program and COPS, standards development in Project 25, Project MESA, NPSTC working groups, and the Software Defined Radio Forum; and acquisition, test and evaluation of Project 25 equipment and interoperability devices.

Program/Organization:	**OLES**

Wireless Data

☑ Ability of users to quickly and transparently establish on-scene wireless data networks that function among data terminals located in on-scene vehicles and among data terminal carried by users into buildings, etc.

On behalf of NIJ's AGILE Program and COPS, standardization of wireless approaches through Internet Engineering Task Force (IETF), the Institute of Electrical and Electronics Engineers Standards Committee 802, Project 25, Project MESA, NPSTC working groups, and the Software Defined Radio Forum; and acquisition, test and evaluation of radio equipment and interoperability devices.

Wireless Data

☑ Ability of on-scene personnel to transparently exchange, as authorized, text, image, and/or video data with other on-site personnel, dispatchers, data resources, etc.

On behalf of NIJ's AGILE Program and COPS, and in conjunction with public safety practitioners and Project MESA, standardization of wireless approaches after defining functional/operational requirements in urban settings for voice, data, image and video. Also, standards efforts through Project 25, NPSTC working groups, and the Software Defined Radio Forum), test and evaluation of prospective standardized approaches, and test and evaluation of standard products.

Wireless Data

☑ Ability to protect the privacy of particular information according to applicable laws and statutes so that it can be accessed only by authorized personnel and data terminals.

On behalf of NIJ's AGILE Program and COPS, standardization in conjunction with Project 25/ TIA TR 8, Software Defined Radio Forum, NPSTC SDR Working Group, GLOBAL, etc. Laboratory test and evaluation of prospective standardized approaches, and test and evaluation of standard products.

Wireless Data

☑ Ability to ensure secure exchange of information.

On behalf of NIJ's AGILE Program standards development through Project 25, Project MESA, NPSTC working groups, and the Software Defined Radio Forum), test and evaluation of prospective standardized approaches (before they are offered to standards committees), and test and evaluation of standard products to determine the degree of interoperability among them.

Wireless Data

☑ Capability of high speed data transfer to allow fast exchange of text, image, and streaming video information.

On behalf of NIJ's AGILE Program and COPS, and in conjunction with Project MESA and IAB, standardization of approaches for transferring critical building information to fixed and mobile sites. Coordination with Project 25, NPSTC working groups, and the Software Defined Radio Forum). Laboratory test and evaluation.

Wireless Data

☑ Ability of transparent on-scene system access to multiple information systems regardless of differing data base system architectures and data formats.

On behalf of NIJ's AGILE Program and COPS, and in conjunction with Project MESA, IAB, and GLOBAL, standardization related to acquiring and transferring building data. Coordination with Project 25, NPSTC working groups, and the Software Defined Radio Forum). Also, test and evaluation of prospective standardized approaches and/or test and evaluation of products and services.

Wireless Data

☑ Ability to remotely access a user's agency/jurisdiction data communications infrastructure when the user roams outside the radio coverage area of the user's agency/jurisdiction infrastructure.

On behalf of NIJ's AGILE Program, standardization through Project 25, Project MESA, NPSTC working groups, and the Software Defined Radio Forum), test and evaluation of prospective standardized approaches (before they are offered to standards committees), test and evaluation of standard products to determine the degree of interoperability among them, and test and evaluation of commercially available and emerging interoperability devices.

Wireless Data

☑ Reliable system operational performance (including fault tolerant to individual system failures, redundant coverage from adjacent sites, full service during routine maintenance, and resistant to impact of catastrophic events).

On behalf of NIJ's AGILE Program, standards development through direct technical support to Project 25/TIA TR8, Project MESA, NPSTC working groups, and the Software Defined Radio Forum), and/or with Standards Development Organizations such Committee T1, ITU, etc. Laboratory research, analysis, test and evaluation of prospective approaches, and test and evaluation of standard products.

Program/Organization:	**OLES**

Wireless Data

☑ Flexible and dynamic system administration (includes administration of on-scene wireless data networks).	On behalf of NIJ's AGILE Program, standards development through direct technical support to Project 25/TIA TR8, Project MESA, NPSTC working groups, and the Software Defined Radio Forum), and/or with Standards Development Organizations such Committee T1, ITU, etc. Laboratory research, analysis, test and evaluation of prospective approaches, and test and evaluation of standard products.

Information Systems

☑ Ability to effectively and efficiently exchange data between agencies/jurisdictions, e.g., by employing common data representation structures and exchange formats and protocols.	On behalf of NIJ's AGILE Program and COPS, standards development through GLOBAL Standards Committees. In particular, the standardization of XML implementation approaches, XML data element dictionary, XML Schema, and Information Sharing Registry. Laboratory support to facilitate specification of standards.

Information Systems

☑ Ability to rapidly access subject information at critical decision points from both field and base locations, including but not limited to information regarding identification (photos, fingerprints, etc.) and activity (criminal history, wants/warrants, reporting/contact history, etc.).	On behalf of NIJ's AGILE Program and COPS, standardization through direct support to GLOBAL Standards Committees, Project 25/ TIA TR 8, Software Defined Radio Forum, and NPSTC SDR Working Group. Laboratory support to facilitate standardization.

Information Systems

☑ Ability to enter information once, then share and reuse that information among all entities that require it.	On behalf of NIJ's AGILE Program, standardization through direct technical support to GLOBAL Committees, and in particular to the standardization of XML implementation approaches, XML data element dictionary, XML Schema, and Information Sharing Registry, and to the standardization of architectural frameworks, and information sharing processes and procedures.

Information Systems

☑ Ability to query/access multiple data sources using one request that is routed to multiple entities simultaneously.	On behalf of NIJ's AGILE Program, standardization through direct technical support to GLOBAL Committees, and in particular to the standardization of XML implementation approaches, XML data element dictionary, XML Schema, and Information Sharing Registry, and to the standardization of architectural frameworks, and information sharing processes and procedures.

Information Systems

☑ Capability of standardized security, including functions and features that can be used to satisfy reasonable security requirements of any entity within a broader security framework.	On behalf of NIJ's AGILE and COPS, standardization support to GLOBAL, and in particular to the standardization of XML implementation approaches, XML data element dictionary, XML Schema, and Information Sharing Registry, and to the standardization of architectural frameworks, and information sharing processes and procedure). In conjunction with GLOBAL, the Federal CIO Council, and XML.gov, development of an effective and efficient security model.

Information Systems

☑ Ability to exchange information with Computer-Aided Dispatch (CAD) systems.	On behalf of NIJ's AGILE Program, standardization through GLOBAL Standards Committees, IEEE 1512 Standards Committee, Project 25 and Project MESA.

Information Systems

☑ Capability of field photo scanning and image file distribution.	On behalf of NIJ's AGILE Program standardization GLOBAL, Project 25, Project MESA, NPSTC working groups, and the Software Defined Radio Forum), test and evaluation of prospective standardized approaches, test and evaluation of standard products to determine the degree of interoperability among them, and test and evaluation of commercially available and emerging interoperability devices.

Program/Organization:	**OLES**

Information Systems

☑ Ability to have near-real-time distribution of text messages to multiple organizations responding to a large event.	On behalf of NIJ's AGILE Program and COPS, standards development and associated laboratory support to GLOBAL Standards Committees, Project 25/ TIA TR 8, Software Defined Radio Forum, NPSTC SDR Working Group, and IEEE 1512.

Information Systems

☑ Ability to access information related to hazardous materials, water sources, floor and building plans, utility maps, weather forecasts, topographic terrain, and other background data that may influence how public safety practitioners approach or conduct operations at an incident.	On behalf of NIJ's AGILE Program and COPS, research and development of wireless transceiver/sensor technologies aimed at providing temporary situational awareness and direct communication links for first responders. Standardization in conjunction with GLOBAL Standards Committees and the InterAgency Board for Equipment Standardization and Interoperability (IAB).

Information Systems

☑ Ability to access medical/treatment records (both those required to ensure proper treatment of incident victims and/or prisoners and those records obtained under warrant).	On behalf of NIJ's AGILE Program, standardization support to GLOBAL Standards Committees, and working groups of the IAB.

Information Systems

☑ Ability to access information regarding pending investigation/litigation of a particular subject.	On behalf of NIJ's AGILE Program and COPS, standards development through GLOBAL Standards Committees, and in particular to the standardization of XML implementation approaches, XML data element dictionary, XML Schema, and Information Sharing Registry, and to the standardization of architectural frameworks, and information sharing processes and procedures.

Information Systems

☑ Ability to access court scheduling information.	On behalf of NIJ's AGILE Program and COPS, standards development through GLOBAL Standards Committees, and in particular to the standardization of XML implementation approaches, XML data element dictionary, XML Schema, and Information Sharing Registry, and to the standardization of architectural frameworks, and information sharing processes and procedures.

Information Systems

☑ Ability to automatically link disposition data with charge data on subject RAP sheet/CCH information.	On behalf of NIJ's AGILE Program and COPS, standards development through GLOBAL Standards Committees, and in particular to the standardization of XML implementation approaches, XML data element dictionary, XML Schema, and Information Sharing Registry, and to the standardization of architectural frameworks, and information sharing processes and procedures.

Information Systems

☑ Capability of automatic dissemination of disposition data to appropriate local, state, and federal agencies/databases.	On behalf of NIJ's AGILE Program and COPS, standards development through GLOBAL Standards Committees, and in particular to the standardization of XML implementation approaches, XML data element dictionary, XML Schema, and Information Sharing Registry, and to the standardization of architectural frameworks, and information sharing processes and procedures.

Information Systems

☑ Ability to access current resource data (including personnel, equipment, materials, etc.) of multiple agencies/jurisdictions responding to a multi-agency/jurisdictional event by authorized users in the respective agencies/jurisdictions.	On behalf of NIJ's AGILE Program and COPS, standardization in conjunction with GLOBAL Standards Committees, IAB, IEEE 1512, and Project MESA.

Program/Organization:	**ONDCP / CTAC**
Full Name:	Office of National Drug Control Policy / Counterdrug Technology Assessment Center
Agencies:	White House
Partnering Agencies / Orgs.:	
Web Page:	http://www.whitehousedrugpolicy.gov/index.
Contact Name:	Al Brandenstein
	Chief Scientist, ONDCP; Director, CTAC
Contact Phone:	1-800-666-3332
Contact Email:	*(see Notes below)
Current Products:	The Technology Transfer Program -- provides, at no cost to agencies, equipment and training for deployments and operations, including telecommunications interoperability equipment (e.g., the ACU-1000). All equipment is transferred to each recipient agency and becomes the permanent property of that organization. ONDCP Clearinghouse: The Clearinghouse is staffed by subject matter specialists and serves as a resource for statistics, research data, and referrals useful for developing and implementing drug policy. The Clearinghouse disseminates ONDCP and the U.S. Department of Justice's Office of Justice Programs (OJP) drug-related publications; writes and produces documents on drug-related topics; coordinates with Federal, state, and local agencies to identify data resources; maintains a reading room offering a broad range of policy-related materials; answers telephone and e-mail requests for information; and provides on-line access to information through ONDCP Web sites.
Planned Products:	
Additional Information:	To send e-mail to Al Brandenstein, Chief Scientist of ONDCP and Director, CTAC, please send the e-mail to ondcp@ncjrs.org, with a request to forward the e-mail to Dr. Brandenstein Additional contact for ONDCP/CTAC: Creigh Yarbrough 202/395-6619 Creigh_Yarbrough@ondcp.eop.gov The U.S. Army Electronic Proving Grounds administers the CTAC Technology Transfer Program.
Program Goals:	The principal purpose of ONDCP is to establish policies, priorities, and objectives for the Nation's drug control program. The goals of the program are to reduce illicit drug use, manufacturing, and trafficking, drug-related crime and violence, and drug-related health consequences. To achieve these goals, the Director of ONDCP is charged with producing the National Drug Control Strategy. The Strategy directs the Nation's anti-drug efforts and establishes a program, a budget, and guidelines for cooperation among Federal, state, and local entities.
Sectors Addressed:	☑ ***Law Enforcement*** ☐ ***Corrections*** ☐ ***EMS*** ☐ ***Military*** ☐ ***Courts*** ☐ ***Probat./Parole*** ☐ ***Emerg. Manag.*** ☐ ***Other***

Program/Organization:	**ONDCP / CTAC**

☐ *Public Defender*	☐ *Fire Protection*	☐ *Transportation*
☐ *Prosecution*	☐ *Public Works*	☐ *Utlities*

Program/Organization:	**ONP**
Full Name:	Office of National Preparedness
Agencies:	Department of Homeland Security, Emergency Preparedness and Response Directorate
Partnering Agencies / Orgs.:	1. State and Local Emergency Agencies 2. 27 Federal Agencies 3. American Red Cross 4. U.S. Fire Administration
Web Page:	http://www.fema.gov/fema/first_res.shtm and www.fema.gov/onp/ncb.shtm
Contact Name:	Gil Jamieson
	Director, Program Coordination Division
Contact Phone:	202-646-4090
Contact Email:	Gil.Jamieson@dhs.gov
Current Products:	FY 2003 Interoperable Communications Equipment Grant Program -- The Emergency Preparedness and Response Directorate (EPR), in the Department of Homeland Security (DHS) and the Department of Justice's Office of Community Oriented Policing Services (COPS) are collaborating on their interoperable communications grant programs in order to maximize the strategic impact of the funding. The funding available this year will not solve the national interoperability problem, but the lessons learned will guide future communications equipment funding so that all purchases meet an interoperability performance standard. EPR and the COPS Office will distribute the funds through a competitive grant program to local jurisdictions across the nation for demonstration projects that will explore uses of equipment and technologies to increase interoperability among the fire service, law enforcement, and emergency medical service communities. In the future, these demonstration projects will serve as models of interoperable solutions that can be shared throughout the nation.
Planned Products:	
Additional Information:	http://www.fema.gov; http://www.dhs.gov Telephone for general information: 202-566-1600
Program Goals:	1. Strengthening the ability of state and local emergency management and response to prepare for and respond to all hazards 2. Building and sustaining a national preparedness and response capability

Sectors Addressed:	☑ ***Law Enforcement***	☐ ***Corrections***	☑ ***EMS***	☐ ***Military***
	☐ ***Courts***	☐ ***Probat./Parole***	☑ ***Emerg. Manag.***	☐ ***Other***
	☐ ***Public Defender***	☑ ***Fire Protection***	☐ ***Transportation***	
	☐ ***Prosecution***	☐ ***Public Works***	☐ ***Utilities***	

Program/Organization:	**Oregon RAINS**
Full Name:	Oregon RAINS (Regional Alliance for Infrastructure and Network Security)
Agencies:	State of Oregon Regional Maritime Security Coalition, Oregon University System, Oregon Economic and Community Development Department, Multnomah County Bureau of Emergency Communications, National Center for Disaster Decision-Making, city of Coquille, OR, Portland Water Bureau, Hillsboro Police RAINS is a public/private partnership and includes private companies
Partnering Agencies / Orgs.:	Communications Security Officials
Web Page:	http://www.oregonrains.org/
Contact Name:	Charlie Kawasaki
	Executive Director
Contact Phone:	503-806-1484
Contact Email:	ck@oregonrains.org
Current Products:	RAINS-NET, a multi-state, Internet-based information technology initiative that is pioneering the use of information-sharing technology on the local level, among critical public and private sector organizations, to improve homeland security. In simplest terms, RAINS-NET is an internet-based online service that enables a trusted community of experts and users involved in Homeland Security and Emergency Management to receive, send, and share sensitive information, and collaborate in near-real time. The information -- which can include training, instructions, breaking event information, coordination, maps, and reports -- remains under control in a "closed" environment. The system is useful even when network connections are unavailable or sporadically available, because the information is transmitted and stored securely on devices such as PCs.
Planned Products:	o Extend RAINS-NET to additional geographic areas o Extend RAINS-NET to additional public safety and homeland security domains
Additional Information:	Contact: Oregon RAINS PMB 384, 25 NW 23rd Place Suite #6 Portland, OR 97210 E-mail: ck@oregonrains.org 503/203-1391 Charles Jennings, Chairman, 503-796-7926 charles.jennings@swanisland.net Eileen Drake, Director of Marketing 503/203-1391 eileendrake@oregonrains.org
Program Goals:	The program, RAINS-NET, is a technology initiative spearheaded by a coalition of Oregon high-tech companies, the Oregon University System, the Oregon Economic and Community Development Department and 911/Emergency Operations Centers. Program goals:

Program/Organization:	**Oregon RAINS**

o An inter-organizational information network to link key public and private organizations in a highly secure, reliable computing environment, in urban and rural environments
o A communications system designed to share sensitive information, alerts, instructions, and rich media across key stakeholders and responders involved in public safety and homeland security
o A communications system that pilots advanced applications for natural disaster and terrorism preparedness, emergency management, and post-event analysis
o A platform for testing and deploying new public safety, homeland security and cybersecurity products and systems -- especially those with value in public sector, critical infrastructure, and first responder IT environments
o A platform for conducting advanced research in key areas deemed critical by organizations such as DHS, OLES, NIST, NSF, and DoD

Sectors Addressed:			
☑ *Law Enforcement*	☑ *Corrections*	☑ *EMS*	☑ *Military*
☐ *Courts*	☐ *Probat./Parole*	☑ *Emerg. Manag.*	☐ *Other*
☐ *Public Defender*	☑ *Fire Protection*	☑ *Transportation*	
☐ *Prosecution*	☑ *Public Works*	☑ *Utlities*	

Functional Capabilities:

Wireless Data

☑ Ability to initiate wireless data communications by requiring the user to only enter (on his/her data terminal/radio) a user identification which authenticates and validates the user, registers and sets data resource capabilities for the user, and completes all radio network administration for the user's data communications with other members of the user's agency/jurisdiction and with other agencies/jurisdictions, as authorized.

RAINS-NET client capabilities require only the existence of an IP signal in order to send and receive information. The USER-ID and password authenticates and binds the user to the local system, then transmits his/her credentials via the IP network to the SWARM server, which then provides specific and targeted information to the authorized user, based on Job Function, Location, Authorization Level, etc.

Wireless Data

☑ Ability of users to quickly and transparently establish on-scene wireless data networks that function among data terminals located in on-scene vehicles and among data terminal carried by users into buildings, etc.

RAINS-NET incorporates SWARM technology, which has been demonstrated in this capacity within the ACTD HLS C2 program and the InfraLynx mobile communications truck. "Scout" clients can quickly link to the local IP infrastructure provided by the mobile communications vehicle and then send/receive relative on-scene information, sharing it with other on-scene participants or transmitting it back to centralized operation centers where it can be authenticated, sanitized, and redistributed.

Wireless Data

☑ Ability of on-scene personnel to transparently exchange, as authorized, text, image, and/or video data with other on-site personnel, dispatchers, data resources, etc.

Scout clients can capture reports that include audio, video, or still images and deliver/publish the contents to other SWARM participants.

Program/Organization:	**Oregon RAINS**

Wireless Data

☑ Ability to protect the privacy of particular information according to applicable laws and statutes so that it can be accessed only by authorized personnel and data terminals.

SWARM supports many content attributes that can be used to target content for specific individuals. These attributes, which are established by the content publisher and verified by a simple and expeditious review process, ensure that only the appropriate users will receive the information. Additionally, it is assumed that some standard policies will be in place restricting the users ability to discuss or interact with the content outside of the SWARM system.

Wireless Data

☑ Ability to ensure secure exchange of information.

Content is always secured when stored and when in transition via networks. All transactions and communications between Scout clients and SWARM "Hive" servers are secured using the Web Services Encryption standard.

Wireless Data

☑ Capability of high speed data transfer to allow fast exchange of text, image, and streaming video information.

The Scout client receives a manifest of information that it should have locally. Scout client only transfers the deltas, or those pieces of information that have changed or are new. Additionally, the Scout client has the intelligence to organize the receipt of information by importance and size. Alerts and incidents receive the highest priority.

Wireless Data

☑ Ability to remotely access a user's agency/jurisdiction data communications infrastructure when the user roams outside the radio coverage area of the user's agency/jurisdiction infrastructure.

RAINS-NET Scout clients are IP based and will work across the public Internet, wireless communications channels or dial-up services. Once a connection is established, the Scout client requests information from the Hive to get updates specific to the users profile.

Wireless Data

☑ Reliable system operational performance (including fault tolerant to individual system failures, redundant coverage from adjacent sites, full service during routine maintenance, and resistant to impact of catastrophic events).

Designed as a public IP network system, SWARM supports load balancing, redundancy, edge content caching, etc. The system is capable of fitting into the most stringent environments.

Wireless Data

☑ Flexible and dynamic system administration (includes administration of on-scene wireless data networks).

Future directions of RAINS-NET SWARM will allow for the dynamic administration of the network and users, and will also provide support for additional communications via blue-tooth, and other wireless protocols.

Information Systems

☑ Ability to effectively and efficiently exchange data between agencies/jurisdictions, e.g., by employing common data representation structures and exchange formats and protocols.

RAINS-NET utilizes standard XML, XACML, common alert protocols, and web services, and supports any SQL compliant database.

Information Systems

☑ Ability to rapidly access subject information at critical decision points from both field and base locations, including but not limited to information regarding identification (photos, fingerprints, etc.) and activity (criminal history, wants/warrants, reporting/contact history, etc.).

RAINS-NET Scout client technology was built for survivability, therefore offline access to information stored locally via the Secure Local Device Caching technology provides the ability to retrieve and review information that may not be reachable in a true crisis (networks down, facilities unavailable, etc.) SWARM technology also provides the ability to securely hook into other 3rd party data sources.

Program/Organization:	**Oregon RAINS**

Information Systems

☑ Ability to enter information once, then share and reuse that information among all entities that require it.	RAINS-NET allows information to be entered once and easily distributed through the content targeting features to authorized participants. More importantly, that information can be pre-positioned prior to general availability, activated and deactivated in real-time, and revoked, pulled back, or replaced without end-user intervention. Information remains controlled by Central Command.

Information Systems

☑ Ability to query/access multiple data sources using one request that is routed to multiple entities simultaneously.	RAINS-NET SWARM technology is a Command and Control model, meaning content is targeted for distribution and then pushed to the end-users. The SWARM Hive is capable of receiving information from multiple sources, automatically targeting that information, and then pushing to all of the affected users.

Information Systems

☑ Capability of standardized security, including functions and features that can be used to satisfy reasonable security requirements of any entity within a broader security framework.	The SWARM system employs the standard AES symmetric cipher for securing all information stored in the system and during the transmission. Web Services Encryption is employed to protect the transactions. Also, the secure local cache is a new and innovative way to ensure that content stored on the end-user's PC is protected and controlled by the SWARM system.

Information Systems

☑ Ability to exchange information with Computer-Aided Dispatch (CAD) systems.	RAINS-NET SWARM can receive and deploy dispatches from multiple sources, automate the targeting of the information and then ensure that the target base receives those notifications. As an example, RAINS-NET is currently working with 911 centers to receive their automated dispatches of emergency personnel and vehicles and then target the information for alert notification to schools, building owners in downtown areas, security personnel, etc.

Information Systems

☑ Capability of field photo scanning and image file distribution.	RAINS-NET Scout client incorporates "Spot Reports," which allows users to report activities, attach audio, video, or still images along with descriptive text. This information is sent back to the Command Center where it can be reviewed and then distributed out for other system users.

Information Systems

☑ Ability to have near-real-time distribution of text messages to multiple organizations responding to a large event.	RAINS-NET technology is not an instant messaging system, but a near real-time distribution of text (and other media when desirable) and alert notifications. SWARMS can be segmented by Work Groups, Job Functions, Authorization Levels, etc. This enables the initiators of events to easily target the base of users that should receive that information.

Information Systems

☑ Ability to access information related to hazardous materials, water sources, floor and building plans, utility maps, weather forecasts, topographic terrain, and other background data that may influence how public safety practitioners approach or conduct operations at an incident.	When the above-named data is entered into RAINS-NET's Hive, the information (in many file formats) is preemptively distributed to a secure cache on the end user's Windows-enabled device, which means the information remains accessible and useful even when the network is down. Also, the user is notified that the information has arrived and should be reviewed.

Information Systems

☑ Ability to access medical/treatment records (both those required to ensure proper treatment of incident victims and/or prisoners and those records obtained under warrant).	Medical records entered into the Hive will be securely delivered to, and accessible by, all properly authenticated users.

Program/Organization:	**Oregon RAINS**

Information Systems

☑ Ability to access court scheduling information.	SWARM supports the ability to push out notifications and schedules as a simple content type to end users.

Information Systems

☑ Capability of automatic dissemination of disposition data to appropriate local, state, and federal agencies/databases.	This type of information is quite easy to automate and distribute using the RAIN-NET SWARM system.

Information Systems

☑ Ability to access current resource data (including personnel, equipment, materials, etc.) of multiple agencies/jurisdictions responding to a multi-agency/jurisdictional event by authorized users in the respective agencies/jurisdictions.	When multiple agencies/jurisdictions have agreed to share information, they do so by publishing information to centralized operation centers containing Hives, where it will be distributed to all authorized users across participating multiple agencies/jurisdictions, whether heterogeneous or homogeneous. There are several mechanisms for supporting the automated delivery and cataloging of this type of information on the end-users Scout client.

Program/Organization:	**PPW**
Full Name:	Partnership for Public Warning - All-Hazard Public Warning System
Agencies:	Open association
Partnering Agencies / Orgs.:	NASA, FEMA, NOAA, NWS, MITRE, Lucent Technologies, others
Web Page:	http://www.partnershipforpublicwarning.org
Contact Name:	Kenneth Allen
	PPW Executive Director
Contact Phone:	
Contact Email:	
Current Products:	1. PPW Report 2002-02, Developing a United All-Hazard Public Warning System 2. PPW Report 2002-01, A Strategy for a national Public Warning System 3. Development of Common Alerting Protocol 4. Definition of Alerting Terminology
Planned Products:	
Additional Information:	
Program Goals:	o Provide a forum to discuss and develop - standards - terminology / definition - technical assessments of systems to provide a national public all-hazard warning system

Sectors Addressed:	☑ ***Law Enforcement***	☐ ***Corrections***	☑ ***EMS***	☑ ***Military***
	☐ ***Courts***	☐ ***Probat./Parole***	☑ ***Emerg. Manag.***	☑ ***Other***
	☐ ***Public Defender***	☑ ***Fire Protection***	☑ ***Transportation***	***Health, CDC***
	☐ ***Prosecution***	☑ ***Public Works***	☑ ***Utlities***	

Program/Organization:	**Project 25**
Full Name:	Public Safety Digital Radio Standard
Agencies:	APCO/NASTD/FED
Partnering Agencies / Orgs.:	Project 25 is a joint effort of Federal, state, and local law-enforcement agencies in areas of wireless land mobile radio (LMR) information technology.
Web Page:	http://www.tiaonline.org/standards/project_25/
Contact Name:	Craig Jorgensen
	Chair, Project 25 Steering Committee
Contact Phone:	801-583-1099
Contact Email:	jorgensen@sisna.com
Current Products:	January 2003 CD ROM of 'Project 25---The TIA-published 102 Series Documents.' The CD ROM contains 33 TIA-102-approved overview documents and technical standards in PDF format on the Project 25 General System Model Interfaces: Common Air, Data Peripheral, Intersystem, Telephone Interconnect, Network Management, and Host and Network. Revised draft interface standards are being developed by the TIA TR-8 Committee. See http://www.tiaonline.org/standards, click on "TR-8".
Planned Products:	
Additional Information:	John Oblak, Chair of TR-8 507/835-6267
Program Goals:	Project 25 goals include standards for obtaining interoperability of radios for Federal, state, and local public-safety agencies, maximizing spectrum efficiency, and fostering competition throughout the life of the radio systems.

Sectors Addressed:	☑ *Law Enforcement*	☑ *Corrections*	☑ *EMS*	☑ *Military*
	☐ *Courts*	☑ *Probat./Parole*	☑ *Emerg. Manag.*	☑ *Other*
	☐ *Public Defender*	☑ *Fire Protection*	☑ *Transportation*	*Forestry, Fish & Wildlife, Parks, Natural Resources*
	☐ *Prosecution*	☑ *Public Works*	☑ *Utlities*	

Functional Capabilities:

Wireless Voice

☑ Ability to initiate wireless voice communications by requiring the user to only enter (on his/her radio) a user identification which authenticates and validates the user, registers and sets talk groups/capabilities for the user, and completes all radio network administration for the user's voice communications with other members of the user's agency/jurisdiction and with other agencies/jurisdictions, as authorized.

Access to P25 network from an authorized subscriber unit is normally automatic. Most conventional systems are open within the limitation of interoperability on both a technology and frequency basis. It is important to remember that inter-jurisdictional communications should be planned for, authorized, and updated as part of the agency's normal planning, implementation, and maintenance process. This requires close cooperation and a great deal of information exchange on a regular and systemized basis.

Wireless Voice

☑ Ability for users to transparently communicate, as authorized, with other members of the agency/jurisdiction on a unit-to-group (one-to-many) basis and a unit-to-unit (one-to-one) basis.

Project 25 networks are designed to accommodate unit-to-unit or unit-to-group communications based on either preplanned inter-communications plans or on dynamic requirements. Pre-definition of talk-groups and inter-relationships is a critical component in the implementation of any advanced telecommunications system, since most of these transactions are handled automatically.

Wireless Voice

☑ Ability of the agency/jurisdiction to administer the priority for voice communications of particular users and particular applications (such as task force operations, incidents, etc.).

The ability to prioritize access and communications within a Project 25 standardized system is based on a user-defined hierarchical structure. Priority on a daily basis is given to those applications, services,and users who have the highest level of access within the predefined levels of access authorization. While priority access is normally predefined, it can be redefined by the user's agency as the need exists. Initial system plans, as well as long-term operational procedures and inter-local agreements, must reflect how these data bases will be changed, by whom, when, and with whose authorization. It is important to note that good engineering practices will help design these advanced systems with enough capacity so that actual use of priority is reserved for extraordinary circumstances, and virtually all users normally obtain immediate access to the system.

Wireless Voice

☑ Ability to communicate an emergency voice message and/or signal which has priority over other voice communications.

Project 25 Statement of Requirements (SoR) and standards were created with the full recognition that priority access was an integral part of the user's specialized requirements. While the concept of ruthless preemption in a digital network is an integral part of the P25 SoR, reality dictates that what is actually taking place is a rapid reallocation of the very first spectrum resource to the requesting unit. An actual effort to override an existing transmission with a new one, no matter how important, would probably mean the demise of both messages.

Wireless Voice

☑ Ability to have secure voice communications.

The Project 25 standards were designed to allow for the use of the Federal government's Type 1, Type 2, and Type 3 encryption algorithms, and also proprietary algorithms. The use of several approved Type 3 encryption algorithms, including DES, Triple-DES,and the AES, are fully specified in Project 25 standards. Type 1 encryption is defined in classified government documents. Users may also choose to use a company's proprietary encryption algorithm with full knowledge of the complications that such a choice may introduce into interoperability.

Wireless Voice

☑ Ability for users to transparently communicate, as authorized, among multiple agencies/jurisdictions some of which may use different technologies, infrastructures and/or frequency bands.

Interoperability between multiple agencies can occur on a number of levels within a Project 25 trunked or conventional network. The first level is through planned access based on inter-local agreements and preprogrammed authorization. It can also occur on a special-needs basis, given certain preplanned conditions are met.

While Project 25 standards are designed to ensure interoperability between standardized technologies, there are also provisions for inter-operability between non-standard analog systems as well as backward compatibility to a company's proprietary, analog trunked system on a manufacturer-by-manufacturer basis.

Even though the same Project 25 standards can be applied in each of the current FCC public safety spectrum allocations bands, there is nothing inherent in the SoR or any of the standards to date that ensures interoperability between bands. That level of service would normally be handled by advanced planning and one of many limited, but very functional, gateway options.

Wireless Voice

☑ Ability to remotely access a user's agency/jurisdiction voice communications infrastructure when the user roams outside the radio coverage area of the user's agency/jurisdiction wireless infrastructure.

Because the Project 25 standards anticipate both roamers from other systems and their units roaming outside of their system, several layers of remote access have been or are in the process of being established. Access to a P25 network by roamers coming into an established network can either be obtained by predefined cooperative agreements, use of pre-planned common calling channels, or through the dual mode (analog - digital) attributes of the technology. Adjacent P25 systems with proper authorization and authentication pre-established in cooperative agreements should be able to inter-communicate through the P25 Inter-Service System Interface (ISSI) once that standard is finalized.

P25 agency subscriber units roaming outside of their network may roam into other standardized networks and obtain the same level of service described above. Once again, non-standardized technology may obtain access through pre-established cooperative arrangements and analog or digital common calling channels, cross-band repeaters, or other types of manual or automated distribution devices. While technology is extremely important in achieving interoperability, success cannot be achieved without comprehensive advance planning and long-term data base and system management.

Wireless Voice

☑ Ability to effectively initiate and sustain flexible and dynamic system administration (includes administration of talk groups, emergency alerts, networks, and channels for mutual aid).

The Project 25 standards are based on the use of SNMP and are specifically set to ensure each user has the opportunity to create and develop their own system management tools within the limitations of the basic application platform. Wireless system management is usually performed on the same platform, using predefined software provided by the equipment supplier.

Wireless Voice

☑ Ability to sustain highly reliable system performance across interconnected systems (including tolerance to individual system failures, redundant coverage from adjacent sites, resistance to impact of catastrophic events, etc).

System reliability, while an integral part of the Project 25 standards process, is in the end more of a function of the system design and implementation of that technology than the technology itself. P25 technology is capable of operating in a conventional mode, trunked mode, simulcast mode or multi-cast mode, depending on the size and scope of the system and its requirements for coverage and services. Trunked standards include the capability for gradual (graceful) degradation. Interoperability between systems will be maintained by the ISSI now under consideration. While yet to be created, the P25 SoR also requires compliant standards for mobile (vehicular) repeaters, which adds another dimension of redundancy. Given massive or catastrophic system failure, the P25 systems standardized to date have the capability of car-to-car, portable-to-portable, or portable-to-car direct mode communications, which also provides another level of communications redundancy for the end users. While all of these attributes are critical to a well-defined network, without comprehensive advanced planning and ongoing system maintenance and operational management, they can expect to perform at something less than the optimal level.

Wireless Voice

☑ Ability to remotely (over-the-air) reprogram a user's radios and/or modify a user's encryption keys and/or modify a radio's waveforms.

Most digital technologies in the marketplace today have the ability to perform predefined levels of what is referred to here as remote rekeying. Project 25 radios are no different. However, before any over-the-air rekeying or re-programming can take place, the end users must be able to define which functions they believe should be accessed over the air, by what authority, and by whom, a problem that is far more complex than it may appear.

Over-the-air rekeying of Project 25 encrypted services is a standard option and is currently undergoing the final standardization and consensus process review. Even though Project 25 radios are capable of a limited "wave-form" conversing with their dual-mode (analog – digital) capability, it is within a well-defined standardized radio. There has not been at this point a P25 attempt or initiative to create a totally dynamic and programmable P25 multi-mode, multi-band product. Such issues as access-defined user access, authentication, operational and service security, antenna compatibilities and system control and management, to name a few, would need to be addressed early on to ensure the proposed multi-mode, multi-band tool would truly benefit and not hinder the users.

Wireless Voice

☑ Ability to provide state-wide (county-wide) signal coverage to vehicular/mobile radios on highways and at street level for state (county) agencies, to provide city-wide signal coverage to portable/handheld radios on the street and within buildings for city agencies, and to provide direct communications between user radios when there is no wireless infrastructure to support communications (such in some rural areas, underground parking garages, and inside some buildings).

Since the P25 standards can be scaled from the very smallest to the very largest system, they can easily be implemented on an area, city, county, state, or national basis. With technology that can operate in the trunked or conventional mode, the use of mobile repeaters (vehicular repeaters), portable repeaters, bi-directional amplifiers/antennas (Bas) and direct mode is inherent in the standards. All standardized portables and mobiles are capable of direct mode communications. A user has the flexibility of having a mixed trunked and conventional system that is deployed based on users needs, population of users, and tasks to be performed. However, once again, it is critical that the users predefine their needs and incorporate them in a comprehensive plan and system design. Finally, the users will need to manage and modify the system over the long term to ensure it meets its maximum potential.

While direct mode (portable-to-portable or mobile-to-mobile) communications is a primary function of a P25 standardized system, the ability to communicate in diverse specialized environments, such as mine shafts and parking garages, is more of a function of the system's design and the defined tactical response for each specialized emergency.

Wireless Data

☑ Ability to initiate wireless data communications by requiring the user to only enter (on his/her data terminal/radio) a user identification which authenticates and validates the user, registers and sets data resource capabilities for the user, and completes all radio network administration for the user's data communications with other members of the user's agency/jurisdiction and with other agencies/jurisdictions, as authorized.

P25 standardized technology is designed to accommodate both voice and data, even though most of the emphasis to date has been on voice services. A conscious decision was made early on in the process that ensures both the users and the creators of the standards clearly understood that data services would be limited by both the limited allocation of spectrum where technology would operate and the concern of the users that emergency voice traffic would not compete with vital data traffic. As a result of that decision, the Project 25 Steering Committee created a separate Statement of Requirements for broadband data, which became known as Project 34. Project 34 eventually evolved into a broadband data specification process, now known as Project MESA.

While the standards are not written to be a primary data transport, the technology can accommodate data. Wireless network access and authentication takes place automatically. The information that is collected by the end users is individually defined, but each transaction carries a detailed identification tag. Network management and operations is normally done with SNMP and with the end users defining their requirements for operational management systems and the network or system provider defining the network management applications. The end users then define their own operational criterion with regard to talk groups, priority of access, and other system attributes. (Note Project 25 Wireless Radio Systems on prior pages.)

Project 25, Phase 1 standards exist to support both packet and circuit switched data but only at the data rate of the Common Air Interface, 9.6 kbps. Phase 2 standards will accommodate higher data rates, but, as discussed previously, wideband data carriage is the subject of Project 24 and Project MESA. All of these are efforts to standardize these technologies. It is apparent that technologies that have been discussed for wideband applications can also be applied to narrow channels, and data rates in the area of 96 kbps in a 25 kHz wide channel are seen as not being too far off.

Wireless Data

☑ Ability of users to quickly and transparently establish on-scene wireless data networks that function among data terminals located in on-scene vehicles and among data terminal carried by users into buildings, etc.

Once again the P25 technology can be used for limited transport of on-scene data within the confines of the originally designed system and the available spectrum resources. Limitations and capabilities with regard to coverage are based more on system design than the actual hardware platform itself.

Wireless Data

☑ Ability of on-scene personnel to transparently exchange, as authorized, text, image, and/or video data with other on-site personnel, dispatchers, data resources, etc.

Since the Project 25 standards are predicated on providing new standardized technologies for narrowband and very narrowband spectrum allocations, its data transport capabilities are restricted by the channel bandwidth. While it is possible to transport text and images, such services must be performed on a noncompetitive basis with critical voice services and in accordance with a well-defined system protocol. Actual coverage will once again be predicated on the user's requirements and the ultimate system design that flows from those requirements. In the long term, it is strongly recommended that voice and data service not be aggregated on narrowband and very narrowband channels except on a limited and defined basis.

Wireless Data

☑ Ability to protect the privacy of particular information according to applicable laws and statutes so that it can be accessed only by authorized personnel and data terminals.

As previously noted, a standardized P25 wireless network has multiple levels of security, including network access and encryptions when it is required.

Wireless Data

☑ Ability to ensure secure exchange of information.

The Project 25 standards were designed to allow for the use of the Federal government's Type 1, Type 2, and Type 3 encryption algorithms, and also proprietary algorithms. The use of several approved Type 3 encryption algorithms including DES, Triple-DES, and the AES are fully specified in Project 25 standards. Type 1 encryption is defined in classified government documents. Users may also choose to use a company's proprietary encryption algorithm with the full knowledge of the complications that such a choice may introduce into interoperability.

Wireless Data

☑ Capability of high speed data transfer to allow fast exchange of text, image, and streaming video information.

Project 25 standardized technologies were never intended to transport high-speed data services.

Wireless Data

☑ Ability of transparent on-scene system access to multiple information systems regardless of differing data base system architectures and data formats.

The standardized P25 network can transport authorized services to any one of a combination of external network interfaces. Routing of that information to specific groups on net would be done by the network controller in accordance with predefined talk-group designations. The host(s) and slaves would be responsible for the routing of the wireless network traffic.

Wireless Data

☑ Ability to remotely access a user's agency/jurisdiction data communications infrastructure when the user roams outside the radio coverage area of the user's agency/jurisdiction infrastructure.

As noted in the wireless voice section, remote roaming and visitor roaming are controlled by a number of factors, in addition to the standardized technology. While the wireless network may allow and authenticate users, the host(s) and the slave(s) authentication must also take place. Network design, implementation, and operation are the controlling factors beyond the technology platform used.

Wireless Data

☑ Reliable system operational performance (including fault tolerant to individual system failures, redundant coverage from adjacent sites, full service during routine maintenance, and resistant to impact of catastrophic events).

Data service transported over a P25 standardized network would be subjected to the same strengths and limitations as voice services but may also meet other barriers in the face of a catastrophic event, since the voice network is primarily self-contained and requires very little if any access to other non-public safety services. Therefore, the level of redundancy and the quality of service is an organization matter under their total jurisdiction and control.

Wireless Data

☑ Flexible and dynamic system administration (includes administration of on-scene wireless data networks).

As previously noted, the P25 standards allow for a great deal of flexibility and dynamic control of the network's authorized users, features, options, and configuration, and reconfiguration. However, given it has limited data transport capabilities in comparison to those really required by the public safety community, benefits to that community may be limited.

Program/Organization:	**Project MESA**
Full Name:	Mobility for Emergency and Safety Applications
Agencies:	North American and European SDOs
Partnering Agencies / Orgs.:	o ETSI (European Telecommunications Standards Institute) o TIA o Public Safety Members, Industry Members (including organized research and support)
Web Page:	http://www.projectmesa.org
Contact Name:	Craig Jorgensen, Chair, Project MESA Service Specifications Group (SSG)
Contact Phone:	801-583-1099
Contact Email:	jorgensen@sisna.com
Current Products:	The Public Safety community (via the SSG) has developed a Statement of Requirements to define needed services and applications. The Project MESA Technical Specifications Group (TSG) has developed a System Reference Model.
Planned Products:	o Specifications for a fully wireless system infrastructure o Specifications for self-establishing, self-healing broadband network operating > 2 Mb/s o Completion of research and technical development on new mechanisms/methods for public-safety communications o Completion of technical specifications by 2004 to revolutionize communications in the public protection/safety and disaster response sectors of the U.S. society.
Additional Information:	John Oblak MESA Steering Committee Chairman (507) 835-6276 MESA Steering Committee Chairman +1.507.835.6276
Program Goals:	o Project MESA is an international partnership whose goal is to produce globally applicable technical specifications for digital mobile broadband technology, aimed initially at the sectors of public safety and disaster response o Project MESA's Service Specification Group is developing the descriptions of services and applications to utilize mobile broadband technology o Project MESA's Technical Specifications Group is developing specifications for the services and application that will be used to develop standards by TIA and by ETSI

Sectors Addressed:				
☑ ***Law Enforcement***	☑ ***Corrections***	☑ ***EMS***	☑ ***Military***
☐ ***Courts***	☑ ***Probat./Parole***	☑ ***Emerg. Manag.***	☑ ***Other***
☐ ***Public Defender***	☑ ***Fire Protection***	☑ ***Transportation***	***Forestry, Fish & Wildlife, Parks, Natural Resources***
☐ ***Prosecution***	☑ ***Public Works***	☑ ***Utilities***	

Functional Capabilities:

Wireless Voice

☑ Ability to initiate wireless voice communications by requiring the user to only enter (on his/her radio) a user identification which authenticates and validates the user, registers and sets talk groups/capabilities for the user, and completes all radio network administration for the user's voice communications with other members of the user's agency/jurisdiction and with other agencies/jurisdictions, as authorized.

Although the Project MESA Statement of Requirements specifically requires interoperability between some existing standardized and proprietary Land Mobile Radio (LMR) services, such as Project 25 and TETRA, in and of itself, is not intended to be a voice LMR communications system. While one of its many primary functions is to be able to support voice communications, those communications services would not normally include public safety dispatch-type service.

In a Project MESA system, the need and dynamics of establishing specific "user grouping" (talk-groups) will depend on the situation at hand and the scope and nature of the emergency being responded to. Inter-agency, agency, inter-jurisdictional and jurisdictional authorization and authentications would either be predefined by inter-local agreements or established on the fly, as may be required to respond to a specific emergency.

Wireless Voice

☑ Ability for users to transparently communicate, as authorized, with other members of the agency/jurisdiction on a unit-to-group (one-to-many) basis and a unit-to-unit (one-to-one) basis.

The SoR for Project MESA specifically requires, and anticipates, the creation of "user grouping" and point-to-point transmission of specific data. It is critical to understand, however, that these transmissions within the MESA network embody voice and many other forms of data applications and services, some of which may not be currently available in the marketplace. Project MESA specifications will be limited to the transport specifications and eventual standards and are not intended to define service applications and protocols.

Wireless Voice

☑ Ability of the agency/jurisdiction to administer the priority for voice communications of particular users and particular applications (such as task force operations, incidents, etc.).

The Project MESA SoR anticipates the need for multiple levels of priority access, bandwidth on demand and a self-healing network. However, since voice communications is an ancillary activity that will generally be directly related to or imbedded in another form of data transport services, it is important to not assume any higher priority will be given to this function than to many of the other functions, unless it has been so defined by the users in the operational data base. It would normally be expected that LMR public safety dispatch-type service would be conducted on an LMR-type network to avoid collisions between voice and other data transmissions.

Wireless Voice

☑ Ability to communicate an emergency voice message and/or signal which has priority over other voice communications.

The Project MESA SoR includes the requirement that all services and users should be capable of being prioritized in accordance with a predefined structure or on a dynamic basis, as may be required to adequately respond to a specific incident.

Wireless Voice

☑ Ability to have secure voice communications.

Even though the Project MESA specifications and eventual standards are not intended to replace traditional public safety LMR services and the specifications and standards have not been written, the SoR clearly articulates the requirements for multiple levels of encryption, which include, but are not limited to, the primary Project 25 standards encryption methods. Those specifications are being created to allow for the use of the U.S. Federal government's Type 1, Type 2, and Type 3 encryption algorithms, and also proprietary algorithms. The use of several approved Type 3 encryption algorithms, including DES, Triple-DES and the AES are fully specified in Project 25 / TIA-102 standards. Type 1 encryption is defined in classified government documents. Users may also choose to use a company's proprietary encryption algorithm with the full knowledge of the complications that such a choice may introduce into interoperability.

We expect other international and national standards will be added to ensure each nation or group of nations choosing to adopt the Project MESA specifications and eventual standards will have the capability to control their own security and protection issues. As a matter of form, it is fully anticipated that end-to-end encryption may be necessary to protect both public records and emergency responder transmissions. Since the information will be in a wireless format, the requirements for full encryption may be even greater than now recognized.

Wireless Voice

☑ Ability for users to transparently communicate, as authorized, among multiple agencies/jurisdictions some of which may use different technologies, infrastructures and/or frequency bands.

The core of the proposed Project MESA specifications and standards is to create a dynamic network that can focus on the transport of bandwidth intensive wireless data services and applications. While transparent access by an authorized MESA user may be allowed based on predefined or dynamically authorized tables, they would not normally be set up for simple voice transaction that could take place on a public safety LMR network or other private or public medium.

Access to different technology platforms and multiple interfaces would depend on the specificity of the final specifications and eventual standards. Nothing in the proposed specifications or standards is intended to imply the Project MESA platform would be spectrum agile and able to intercommunicate with other technology platforms across a wide range of spectrum allocations or bands.

Wireless Voice

☑ Ability to remotely access a user's agency/jurisdiction voice communications infrastructure when the user roams outside the radio coverage area of the user's agency/jurisdiction wireless infrastructure.

The SoR does not anticipate roaming functions as might be expected in a traditional public safety LMR, cellular or personal communications service. In fact, it is anticipated the eventual network specification and eventual standards will be very structured and closely controlled to ensure maximum benefit to the emergency responders, a minimum of threats to security and maximum use of the original investment by making certain that the public safety agencies who cooperated to build the network have access to it when and if they need it. Transient users will be authorized high-speed transport access on an as-needed basis to respond to a specific emergency. Inter-agency voice communications would not normally be considered one of the primary services that a transient unit may require. The users' Project MESA network implementation plan would include "gateways" to other transport services to accommodate users who were outside the network but need to transmit or receive data from the network. The details, issues, and problems associated with those "gateways" have not yet been addressed.

Wireless Voice

☑ Ability to effectively initiate and sustain flexible and dynamic system administration (includes administration of talk groups, emergency alerts, networks, and channels for mutual aid).

The proposed Project MESA specifications may include the need for a large, contiguous piece of spectrum bandwidth, which would be allocated on demand. While the networks that will be derived from the Project MESA specifications will be very flexible and dynamic and have "user groupings" as may be required, it would not normally be used for emergency alerting or traditional mutual aid channels. Mutual aid communications on a Project MESA network may take many non-traditional forms, such as dissemination of video, complex graphical information, and other date intensive files that are related to a specific incident or project.

Wireless Voice

☑ Ability to sustain highly reliable system performance across interconnected systems (including tolerance to individual system failures, redundant coverage from adjacent sites, resistance to impact of catastrophic events, etc).

Since Project MESA is based on a non-traditional set of criteria, redundancy requirements are limited by the scope of the design and requirements of the end user and by how much of the network is terrestrial or extra-terrestrial and how much of it will be fixed sites versus temporary sites. More importantly, the complexity of ensuring a stable environment requires a far more complex design and implementation strategy, and operational procedures. Linkage outside the defined network would only occur on a preplanned or predefined basis unless an interface to some other network was included in the installed base. In any event, it will be highly reliable and highly redundant and serve a multitude of emergency and some traditional high-speed data services.

Wireless Voice

☑ Ability to remotely (over-the-air) reprogram a user's radios and/or modify a user's encryption keys and/or modify a radio's waveforms.

The use of Over-The-Air-Re-Keying (OTAR) and over-the-air subscriber unit updates will no doubt be possible; however, as of this point in the process, no specific applications, features, or functions have been identified.

Wireless Voice

☑ Ability to provide state-wide (county-wide) signal coverage to vehicular/mobile radios on highways and at street level for state (county) agencies, to provide city-wide signal coverage to portable/handheld radios on the street and within buildings for city agencies, and to provide direct communications between user radios when there is no wireless infrastructure to support communications (such in some rural areas, underground parking garages, and inside some buildings).

The requirements outlined in this question are generally more applicable to LMR service. However, given the importance of data and, in the case of Project MESA, high-speed data, it is important to at least provide a general comparison of how those requirements fit with the requirements of the Project MESA SoR. The core of the Project MESA SoR is based on the anticipation that the specifications and eventual standards would, in fact, be capable of providing wide-area coverage, in-building coverage, coverage from moving vehicles and coverage on a city-wide, county-wide and, in some cases, statewide basis. The issue of Project MESA coverage will be founded more on public policy and cost-related issues than on technology. Given the complexity of the technology, it is anticipated that primary or fixed service will be created in major urban areas while secondary, occasional service will be established on an as-needed basis at local hot spots. Since the actual system and service costs are unknown at this phase, much of the actual data relating to implementation will need to wait until a future date.

Program/Organization:	**Project MESA**

Wireless Data

☑ Ability to initiate wireless data communications by requiring the user to only enter (on his/her data terminal/radio) a user identification which authenticates and validates the user, registers and sets data resource capabilities for the user, and completes all radio network administration for the user's data communications with other members of the user's agency/jurisdiction and with other agencies/jurisdictions, as authorized.

Project MESA is a cooperative effort between the public safety communities in North America and Europe, the Telecommunications Industry Association (TIA), and the European Telecommunications Standards Institute (ETSI) to create wireless, broadband, technology specifications and eventual standards that can be used for the transmission of complex data, including voice, video, complex images, and other public safety and first responder files. Please see the Project MESA Statement of Requirements, Requirements Matrix, and Project MESA scenarios on the Project MESA web site at www.projectmesa.org. The Project MESA SoR is based on the concept of providing automatic network access to all authorized subscriber units. Access codes and user identifications are preprogrammed into each unit. Encrypted units would require additional data verification throughout their transmission. Conceptually, the proposed Project MESA technology would initiate the data transaction, verify authentication, and connect all predefined units in the specified user group. Error detection and barriers to unauthorized intrusion would normally be expected. Authorized users would be predefined and established in both the network and authorization tables. The limited number of roaming users that could be expected to join the network would need to establish authority and obtain both an electronic and formal system manager authorization to join the network.

Wireless Data

☑ Ability of users to quickly and transparently establish on-scene wireless data networks that function among data terminals located in on-scene vehicles and among data terminal carried by users into buildings, etc.

At the foundation of Project MESA is the concept of being able to quickly establish wireless, high-speed, ad hoc networks that would allow first responders and others full access to any of the technological resources they may have in their automated tool box. Not only does the SoR stipulate the need for these pre-defined automated accesses, but it ensures that the end users will have the bandwidth they need to accomplish the missions, as they are automatically defined, by the end terminal device. Since MESA is a transport service, its total function is to identify authorized users, authenticate their access, identify their routing table, access their routing table, authenticate that access, identify the appropriate interface, connect to that interface, authenticate access approval, validate handshake has taken place, provide error checking and transmit the payload. As the transaction continues, it is expected that MESA will adjust the bandwidth and associated transport needs to meet the needs of its predefined or dynamically adjusted table of priorities and their demands to access the services.

Wireless Data

☑ Ability of on-scene personnel to transparently exchange, as authorized, text, image, and/or video data with other on-site personnel, dispatchers, data resources, etc.

The Project MESA SoR specifically recognizes the importance of on-scene communications and the transmission of complex images, video, and other network intensive traffic. In fact, the purpose of Project MESA is to create standardized technologies that puts this resource in the hands of the first responders so they can not only communicate with their subordinates, peers, supervisors, supporting agencies, and subject matter experts, they can show an exact vision of what is taking place and what the obstacles are or may be. It is anticipated that the MESA technology will control remote robotics, snuffers, infra-red cameras, robotic bomb disarming devices, and much, much more.

Wireless Data

☑ Ability to protect the privacy of particular information according to applicable laws and statutes so that it can be accessed only by authorized personnel and data terminals.

The Project MESA SoR has established very high requirements with regard to the protection and security of information transported over that network. During our April 2003 Project MESA meeting, the management of the U.S. Federal Government's Public Safety Wireless Network (PSWN) submitted a proposal to the Service Specification Group (SSG) for inclusion of the existing Federal encryptions standards embodied in Type 1, Type 2, Type 3, and AES P25-TIA-102 Standards and Technical Service Bulletins in the proposed Project MESA specifications. That proposal was approved by the MESA SSG and forwarded to the Project MESA Steering Committee (SC), who also approved it and returned it to the Technical Specifications Group(s) for their drafting into a Project MESA specification and eventual standards.

Wireless Data

☑ Ability to ensure secure exchange of information.

Project MESA participants recognize the responsibility to the public and to the public safety field personnel that the new standardized technology will serve. Therefore, they are making every effort to ensure an extremely high level of security and threat protection for both its wireless networks and the terminals that serve on that network. Every consideration is being given these issues as the Project MESA process moves forward. For example, it has already been proposed that the existing Project 25 encryption be incorporated in Project MESA. These standards were designed to allow for the use of the Federal government's Type 1, Type 2, and Type 3 encryption algorithms, and also proprietary algorithms. The use of several approved Type 3 encryption algorithms, including DES, Triple-DES and the AES, are fully specified in Project 25 standards. Type 1 encryption is defined in classified government documents. Users may also choose to use a company's proprietary encryption algorithm with full knowledge of the complications that such a choice may introduce into interoperability.

Wireless Data

☑ Capability of high speed data transfer to allow fast exchange of text, image, and streaming video information.

Project MESA technology will transmit at data rates in excess of 2 mega bits. The applications to be transmitted will include, but not be limited to, full-motion black and white and color video, complex graphics, complex images, detailed data files, and very large text files. These files will be accessible to and from host(s), mobile(s), and portable subscriber units.

Wireless Data

☑ Ability of transparent on-scene system access to multiple information systems regardless of differing data base system architectures and data formats.

The founders of Project MESA fully anticipate that since it is simply a transport vehicle it can and will include the necessary interfaces and protocol conversion tables to access any predefined outside network or host front-end processor. The key will be for the users to identify those applications, services, networks, and protocols early on so they can be prioritized as to work effort and importance to the community at large. (Note Attachments A & B of the Project MESA SoR at www.projectmesa.org.)

Wireless Data

☑ Ability to remotely access a user's agency/jurisdiction data communications infrastructure when the user roams outside the radio coverage area of the user's agency/jurisdiction infrastructure.

As noted previously, the Project MESA SoR does not anticipate roaming functions as might be expected in a traditional LMR, cellular, or personal communications service. In fact, it is anticipated the future network specification and eventual standards will be very structured and closely controlled to ensure maximum benefit to the emergency responders, a minimum of threats to system security, and maximum use of the original investment by making certain that those who are paying for the service have access to it when and if they need it. Transient users will be authorized high-speed transport access on an as-needed basis to respond to a specific emergency. Inter-agency voice communications would not normally be considered one of them. The Project MESA network implementation plan would include "gateways" to other transport services to accommodate users who were outside the network but need to transmit or receive data from the network. The details, issues, and problems associated with those "gateways" have not yet been addressed.

Wireless Data

☑ Reliable system operational performance (including fault tolerant to individual system failures, redundant coverage from adjacent sites, full service during routine maintenance, and resistant to impact of catastrophic events).

While the issue of network reliability hinges as much on the network plan, design, implementation, and operational maintenance and management as it does on the technology platform, the Project MESA SoR has established very high technical requirements to ensure very secure, robust service is always available to the first responder, either on a fixed basis or a "Hot-Spot" basis, as may be required by the incident and those who respond to it. (Please note Project MESA SoR at www.projectmesa.org).

Wireless Data

☑ Flexible and dynamic system administration (includes administration of on-scene wireless data networks).

The Project MESA SoR is predicated on a fully digital transport system, which has aggregated a number of telecommunications services into what is generally classified as "data". Those "data" services would include, but not be limited to, voice, traditional data services, text files, slow scan and full-motion black and white and color video, complex graphics, complex images, data from sensors and monitors, data regarding velocity, density, chemical components, texture and many other data files and services. It is anticipated any or all of these services can be transmitted on a peer-to-peer, peer-to-group, peer-to-host(s) or dispatch center or group-to-group or any other combination of the above, assuming proper authorization and either dynamic programming or preprogramming of users and system identifications (IDs) has taken place. Finally, it is assumed that proper system planning and design preceded the initial installation.

Program/Organization:	**PSWN Program**
Full Name:	Public Safety Wireless Network (PSWN) Program
Agencies:	U.S. Department of Justice U.S. Department of Homeland Security
Partnering Agencies / Orgs.:	Federal, state, and local public safety communities
Web Page:	www.pswn.gov; www.publicsafetywins.gov
Contact Name:	Julio "Rick" Murphy (DHS) and Robert E. Lee, Jr. (DOJ) Co-Program Managers, PSWN
Contact Phone:	1-800-565-PSWN
Contact Email:	Information@pswn.gov

Current Products:

1. INTEROPERABILITY ASSISTANCE
- Provided direct interoperability planning support agencies in nearly 20 states and regions
- Supported the creation of 11 state interoperability committees
- Assisted in the development of statewide system strategies in 10 states
- Conducted regional assessments of existing radio systems (e.g., coverage, requirements)

2. PILOT PROJECTS
- Defined and analyzed 15 unique technical interoperability solutions
- Assessed public safety requirements and implemented technical interoperability solutions in 10 regions across the Nation

3. PUBLIC SAFETY WIRELESS INTEROPERABILITY NATIONAL STRATEGY (WINS)
- Designed a roadmap for improving interoperability consisting of technical and policy - oriented interoperability solutions
- Implemented an interactive Web site that serves as a decision support tool aligning appropriate solutions with user needs
- Captured the first-ever snapshot of the state of interoperability across the Nation

4. INTEROPERABILITY STUDIES
- Provided analysis and recommendations on communications in September 11, 2001, Pentagon attack
- Initiated an after-action report to evaluate interoperability during the DC sniper attacks
- Performed an analysis of statewide and regional systems across the Nation

5. OUTREACH
- Executed 27 symposiums and conferences educating more than 4,500 public safety officials
- Developed 25 high-profile documents, distributed to more than 125,000 public safety officials
- Created Web site and call center that handle 35,000 visits and 1,000 calls/e-mails a year

Planned Products:

1. Completion of interoperability assistance in an additional 13 states
2. Completion of pilot project implementations in Washington, DC, the New Orleans/Baton Rouge region, and the greater St. Louis area
3. Collection of operational and system data in the top 25 homeland security high-threat metropolitan areas to support interoperability solution planning and implementation

Program/Organization:	**PSWN Program**
	4. Determine potential technical solutions for integrating proprietary commercial communications systems with land mobile radio (LMR) systems (iDen-to-LMR) 5. Perform an in-depth analysis of existing radio coverage along the U.S.–Canadian border 6. Construct new tools in Public Safety WINS for evaluating national progress against identified needs 7. Educate more than 1,000 stakeholders on interoperability via new conferences and symposiums
Additional Information:	Julio "Rick" Murphy (DHS), PSWN Program Manager, 703.279.2037, rick.murphy@cio.treas.gov Robert E. Lee, Jr (DoJ), PSWN Program Manager, 703.279.2007, springfield01@earthlink.net
Program Goals:	1. Ensure seamless, coordinated, and integrated public safety communications for the safe, effective, and efficient protection of life and property 2. To plan for and foster interoperability among wireless networks that meet the requirements of local, state, federal, and tribal public safety agencies

Sectors Addressed:	☑ *Law Enforcement*	☐ *Corrections*	☑ *EMS*	☐ *Military*
	☐ *Courts*	☐ *Probat./Parole*	☑ *Emerg. Manag.*	☐ *Other*
	☐ *Public Defender*	☑ *Fire Protection*	☑ *Transportation*	
	☐ *Prosecution*	☑ *Public Works*	☑ *Utlities*	

Functional Capabilities:

Wireless Voice

☑ Ability for users to transparently communicate, as authorized, with other members of the agency/jurisdiction on a unit-to-group (one-to-many) basis and a unit-to-unit (one-to-one) basis.	This capability is addressed as a component of Voice Communications--Functional Area #6 that reads "Ability for users to transparently communicate, as authorized, among multiple agencies/jurisdictions some of which may use different technologies, infrastructures and/or frequency bands."

Wireless Voice

☑ Ability to communicate an emergency voice message and/or signal which has priority over other voice communications.	The PSWN Program is collaborating with the National Communications System (NCS) to test the applicability of Wireless Priority Service (WPS) in emergency public safety land mobile radio (LMR) environments. Public safety responders will benefit by understanding how they can integrate priority wireless voice via WPS with standard LMR, what challenges and options exist for deployment (e.g., interference issues and technical application scenarios), and how to incorporate support for such services into current operations.

Wireless Voice

☑ Ability to have secure voice communications.	The PSWN Program has extensive experience in addressing secure voice communications, including assessing the security of voice networks, implementing security measures in those same systems, and ensuring system security features are adequately addressed by standards-setting bodies. The program has also developed an LMR risk assessment methodology, as well as security planning and policy templates that can be applied to any LMR system. These templates are serving as "de facto" standards for security planning and are key elements in system buildouts at the Departments of Justice and Treasury and in states such as Michigan.

Wireless Voice

☑ Ability for users to transparently communicate, as authorized, among multiple agencies/jurisdictions some of which may use different technologies, infrastructures and/or frequency bands.

Actively addressing interoperability -- the ability for public safety responders to talk to each other by radio seamlessly and in real time -- is central to the PSWN Program mission. The program actively works with local, state, Federal, and tribal public safety agencies to improve spectrum availability, funding, technology and standards, security, and agency coordination. The program has compiled its knowledge gained through implementation activities into a national strategy for improving interoperability, known as Public Safety WINS: Wireless Interoperability National Strategy. The strategy provides a comprehensive multimedia tool and interactive Web site (http://www.publicsafetywins.gov) that helps users identify technical and policy solutions for addressing their specific interoperability needs. Other program activities include providing direct implementation assistance to public safety agencies, conducting operational pilot deployment to address specific state and local needs, and disseminating critical high-profile guides on issues and solution approaches.

Wireless Voice

☑ Ability to remotely access a user's agency/jurisdiction voice communications infrastructure when the user roams outside the radio coverage area of the user's agency/jurisdiction wireless infrastructure.

The PSWN Program has conducted studies and piloted solutions in several geographically diverse regions across the Nation. The solutions have proven to provide best practices that enhance radio coverage and interoperability among multiple public safety agencies from differing agencies and jurisdictions

Wireless Voice

☑ Ability to effectively initiate and sustain flexible and dynamic system administration (includes administration of talk groups, emergency alerts, networks, and channels for mutual aid).

The PSWN Program has assessed dynamic system administration techniques to improve on-scene interoperability. The program has examined the issue from a number of perspectives ranging from the development of an operational best practices report, a "How-To" guide, and various project "after-action" reports (e.g., Capitol Wireless Integrated Network [CapWIN] and Project MESA). The program has been able to educate public safety agencies and their system administrators on ways to improve interoperability through more efficient system management.

Wireless Voice

☑ Ability to sustain highly reliable system performance across interconnected systems (including tolerance to individual system failures, redundant coverage from adjacent sites, resistance to impact of catastrophic events, etc).

The PSWN Program, in collaboration with the NCS, is participating in a reliability assessment for a state public safety 800MHz LMR network. The effort will evaluate the interdependencies between the state system and the Public Switched Telephone Network (PSTN), identify potential points of failure across infrastructures, and provide relevant mitigation strategies. The objective is to provide the state agency with valuable information that can be used to improve the reliability and redundancy of its public safety system infrastructure.

Wireless Voice

☑ Ability to remotely (over-the-air) reprogram a user's radios and/or modify a user's encryption keys and/or modify a radio's waveforms.

The PSWN Program developed analyses and educational materials on two emerging software applications to improve interoperability:

- Securing voice radio transmissions (i.e., over-the-air encryption key management, or over-the-air rekeying [OTAR])

- Manipulating radio frequency transmissions at the waveform level (i.e., software enabled radios [SER]).

The educational materials resulting from these analyses help system planners more effectively implement cost-efficient solutions and plan for longer term interoperable system enhancements.

Program/Organization:	**PSWN Program**

Wireless Voice

☑ Ability to provide state-wide (county-wide) signal coverage to vehicular/mobile radios on highways and at street level for state (county) agencies, to provide city-wide signal coverage to portable/handheld radios on the street and within buildings for city agencies, and to provide direct communications between user radios when there is no wireless infrastructure to support communications (such in some rural areas, underground parking garages, and inside some buildings).	The PSWN Program has provided support to improve signal coverage both in metropolitan (e.g., Washington, DC) and rural areas (e.g., Washington state), and in uniquely challenging geographic areas (e.g., subway system tunnels and rugged coastal terrain). The program has also addressed the ability of laws, regulations, and ordinances to affect the development of in-building wireless systems in urban areas.

Wireless Data

☑ Ability of users to quickly and transparently establish on-scene wireless data networks that function among data terminals located in on-scene vehicles and among data terminal carried by users into buildings, etc.	The PSWN Program has assessed on-scene wireless mobile data networks and their role in improving interoperability. Specifically, the program has assisted with the deployment of a wireless mobile data system (i.e., CapWIN), participated in the development of global standards (i.e., Project MESA), evaluated emerging technologies (e.g., Wireless Firefighter Lifeline [WFL]), and examined wireless data networking standards (e.g., 802.11). As a result, agencies are able to identify and implement appropriate standards and access a collection of data from across several interoperability-focused programs.

Wireless Data

☑ Ability of on-scene personnel to transparently exchange, as authorized, text, image, and/or video data with other on-site personnel, dispatchers, data resources, etc.	The PSWN Program has analyzed the secure exchange of data transmissions among first responders. Specifically, the program has evaluated new data transmission devices (i.e., handheld devices), investigated emerging data transmission technologies (e.g., Telegeoprocessing), and assessed commercial wireless data services. Through in-field experience, the program has also collected information related to on-scene wireless data exchange. In aggregate, these resources enable public safety officials to make more informed technology decisions.

Wireless Data

☑ Ability to ensure secure exchange of information.	The PSWN Program has influenced the future of public safety wireless data security. Specifically, operational testing has enabled the program to determine the suitability of secure technologies for public safety (i.e., secure two-way paging). Contributions to Project MESA wireless data standards will help to shape and define international wireless data security requirements. Lastly, the program's examination of emerging secure technologies (i.e., biometrics) has equipped the public safety community with the information necessary to make sound technology decisions in the future.

Wireless Data

☑ Capability of high speed data transfer to allow fast exchange of text, image, and streaming video information.	The PSWN Program has analyzed many emerging technologies that support high-speed, large-bandwidth transmissions. The program sought to validate claims that these new technologies would enhance public safety communications and operations through detailed technical reviews and analysis. Based on these analyses, agencies are now prepared to select the technologies, as they become commercially available, that best fit their organizational and operational needs.

Program/Organization: **PSWN Program**

Information Systems

☑ Ability to rapidly access subject information at critical decision points from both field and base locations, including but not limited to information regarding identification (photos, fingerprints, etc.) and activity (criminal history, wants/warrants, reporting/contact history, etc.).

The PSWN Program partnered with the FBI Wireless Applications Test Program (WATP) to assess data access systems and determine best practices/lessons learned from "real-world" operations. As a result, the program developed a practical guide for law enforcement first responders on establishing rapid data access. Law enforcement responders now have a resource available through the PSWN Program Web site for establishing access to subject data (e.g., fingerprints, crime reports, and mug shots) internally and through external databases such as the National Crime Information Center (NCIC).

Information Systems

☑ Ability to have near-real-time distribution of text messages to multiple organizations responding to a large event.

The PSWN Program tested and piloted the real-time distribution of text messages using secure paging technology. Paging functionality was demonstrated and the technology was employed in support of agencies involved in the 2002 Winter Olympics in Salt Lake City, UT. The two-way paging solution provided an option for immediate and quick dissemination of critical information to Olympic venue commanders and key personnel.

Information Systems

☑ Ability to access current resource data (including personnel, equipment, materials, etc.) of multiple agencies/jurisdictions responding to a multi-agency/jurisdictional event by authorized users in the respective agencies/jurisdictions.

The PSWN Program has conducted (and is currently conducting) several activities requiring extensive data collection, resulting in the need to make resource data available on a large scale. Customized central databases serve as a single reference source for relevant information (e.g., spectrum used and types of fixed and user equipment deployed). Currently, the program is supporting the development of an extensive database of information for public safety agencies covering the U.S. northern border with Canada.

Program/Organization:	**RISS**
Full Name:	Regional Information Sharing Systems
Agencies:	U.S. DoJ's BJA
Partnering Agencies / Orgs.:	
Web Page:	http://www.iir.com/RISS/
Contact Name:	George March
	Director, RISS Office of Information Technology
Contact Phone:	610-873-9940
Contact Email:	gmarch@risstech.riss.net

Current Products:

In order to facilitate the sharing and exchange of critical information, RISS operates the RISS Secure Intranet (riss.net), a nationwide Sensitive But Unclassified (SBU) secure communications and information sharing network for local, state, Federal, and tribal law enforcement and criminal justice member agencies. RISS operates the only secure Web-Based nationwide network (riss.net) for communication and exchange of criminal intelligence. Services are provided to over 6,300 criminal justice agencies in the 50 states, the District of Columbia, U.S. territories, Canada, England, and Australia, with membership continuing to grow.

By establishing the RISS Anti-Terrorism Information Exchange (RISS ATIX) Program, RISS has expanded accessibility to the RISS Secure Intranet (riss.net) to deliver secure inter-agency communication, information sharing, and dissemination of national security, disaster, and terrorist threat information to an additional group of users. Individuals, referred to as RISS ATIX "participants", include executives and officials from government and non-government "communities" with responsibility for planning and implementing prevention, response, mitigation, and recovery efforts regarding terrorism and disasters. As appropriate to their roles and responsibilities within and among their affiliated communities, RISS ATIX participants are provided access to specific resources available via the RISS Secure Intranet (riss.net). RISS ATIX "communities" are those government and non-government organizational entities whose executives and officials are, in the sense of "public safety", responsible for planning and implementing prevention, response, mitigation, and recovery efforts regarding terrorism and disasters.
The RISS Intelligence Centers provide a number of services to member agencies, including:
o Information sharing
o Telecommunications services
o Analytical and intelligence services
o Investigative support
o Confidential funds
o Specialized equipment
o Specialized training
o Publications and bulletins

RISS resources available electronically via the RISS Secure Intranet (riss.net) include:

Program/Organization:	**RISS**
	o RISS Criminal Intelligence Database Pointer Systems (RISSIntel & RISSNET II) o RISS Investigative Leads Bulletin Board (RISSLeads) o RISS National Gang Database (RISSGang) o Electronic linking to node partner systems and other information resources o RISSSearch o RISSTraining o TechPage o Secure e-mail RISS ATIX resources include: o RISS ATIX Bulletin Board o RISS ATIX Web Site with individual community web pages o Secure e-mail
Planned Products:	RISS has a number of on-going initiatives and continues to research technologies and information sharing concepts that would enhance and augment the capabilities and resources provided via the RISS Secure Intranet (riss.net) infrastructure. Research and development are continuing in the areas of: o Off-line notification of time sensitive alerts and information o Use of secure Instant Messaging in the RISS environment o Expansion of secure Chat features in the RISS environment o Development of secure web conferencing with whiteboard functionality Additionally, RISS continues to develop relationships with other Sensitive But Unclassified (SBU) systems in order to enhance and expand the ability to share sensitive and timely information in a secure manner.
Additional Information:	RISS provides technology resources and the RISS secure intranet (riss.net) infrastructure to enable the integration and electronic connection of member agency law enforcement information technology systems as nodes on riss.net. RISS node partners include the High Intensity Drug Trafficking Area (HIDTA) Investigative Support Centers, the Southwest Border States Anti-Drug Information System (SWBSADIS), the El Paso Intelligence Center (EPIC) Clandestine Laboratory Seizure System (CLSS), and a number of state law enforcement information technology systems. The RISS Secure Intranet (riss.net) is the secure infrastructure providing the communications backbone for implementation of the Multistate Anti-TeRrorism Information Exchange (MATRIX) project. The goal of the MATRIX project is to increase and enhance the exchange of sensitive terrorism information and other criminal activity information between local, state, and Federal agencies. The project leverages and integrates existing and proven technology to provide a new capability to assist law enforcement in identifying and analyzing terrorist and other criminal activity, and appropriately disseminating information to law enforcement agencies nationwide in a secure, efficient, and timely manner. The project has three (3) primary objectives: 1. Use factual data analysis from existing data sources and data integration technology to improve the usefulness of information contained in multiple types of document storage systems 2. Provide a mechanism to become nodes on the RISS secure intranet (riss.net) for electronic information exchange among participating agencies 3. Encourage the exchange of information via secure state Web sites Additional contact: Tony Rispoli, Sr. Project Coordinator, RISS 610-873-9940

Program/Organization:	**RISS**
Program Goals:	The overall objective of the RISS Program is to enhance the ability of local, state, federal, and tribal law enforcement and criminal justice agencies to identify, target, and remove criminal conspiracies and activities spanning multi-jurisdictional, multi-state, and sometimes international boundaries, and to support investigation and prosecution efforts against terrorism, narcotics trafficking, organized crime, criminal gangs, cybercrime, and violent crime. The terrorist attacks of September 11, 2001, caused a dramatic expansion of RISS services to address the need for secure exchange of terrorism information and to provide rapid access to alerts on homeland security matters among all levels of law enforcement, as well as to executives and officials from government and non-government communities responsible for planning and implementing prevention, response, mitigation, and recovery efforts regarding terrorism and disasters.

Sectors Addressed:				
☑ *Law Enforcement*	☑ *Corrections*	☑ *EMS*	☑ *Military*
☑ *Courts*	☑ *Probat./Parole*	☑ *Emerg. Manag.*	☐ *Other*
☑ *Public Defender*	☑ *Fire Protection*	☑ *Transportation*	
☑ *Prosecution*	☑ *Public Works*	☑ *Utlities*	

Functional Capabilities:

Information Systems

☑ Ability to effectively and efficiently exchange data between agencies/jurisdictions, e.g., by employing common data representation structures and exchange formats and protocols.	RISS utilizes and distributes the RISS Extensible Markup Language (XML) Data Exchange Specification (RISSDES) to facilitate electronic integration and information sharing between RISS and riss.net node agency partners.

Information Systems

☑ Ability to rapidly access subject information at critical decision points from both field and base locations, including but not limited to information regarding identification (photos, fingerprints, etc.) and activity (criminal history, wants/warrants, reporting/contact history, etc.).	RISS provides secure access to all resources available via the RISS Secure Intranet (riss.net) to authorized riss.net users from both field (remote user) and base (riss.net node) locations.

Information Systems

☑ Ability to enter information once, then share and reuse that information among all entities that require it.

Information Systems

☑ Ability to query/access multiple data sources using one request that is routed to multiple entities simultaneously.	Multiple data sources available via the RISS Secure Intranet (riss.net) may be queried/accessed by authorized riss.net users with one request that is simultaneously routed to multiple data sources through use of RISSSearch, a master (federated) search tool developed within RISS. Additionally, intelligence database pointer systems available via the RISS Secure Intranet (riss.net) may be queried/accessed with one request.

Program/Organization:	**RISS**

Information Systems

☑ Capability of standardized security, including functions and features that can be used to satisfy reasonable security requirements of any entity within a broader security framework.	RISS deploys standardized network security measures and policies for any member agency information technology system approved for establishment as a node to the RISS Secure Intranet (riss.net). The RISS Secure Intranet (riss.net) authentication and access control technology and methodology allow the resource owner (RISS Intelligence Centers and node partners) full control of access to and use of their specific resource.

Information Systems

☑ Capability of field photo scanning and image file distribution.	Various types of media files, including but not limited to .jpg, .bmp, .gif, .avi, .doc, and .ppt files, can be distributed over the RISS Secure Intranet (riss.net) and posted to specific RISS resources.

Information Systems

☑ Ability to have near-real-time distribution of text messages to multiple organizations responding to a large event.	The RISS Secure Intranet (riss.net) provides the capability for distribution of text messages to multiple users via e-mail to any device used to access riss.net capable of receiving e-mail messages.

Program/Organization:	**S&T Directorate**
Full Name:	Science and Technology Directorate
Agencies:	Department of Homeland Security
Partnering Agencies / Orgs.:	1. Border and Transportation Security workers 2. Emergency Preparedness and Response community 3. CBRNC workers 4. Information Analysis & Infrastructure workers
Web Page:	http://www.dhs.gov/dhspublic/contactus http://www.whitehouse.gov/deptofhomeland/
Contact Name:	Holly Dockery
	Director, Standards/State and Local
Contact Phone:	202-786-0076
Contact Email:	holly.dockery@dhs.gov
Current Products:	1.Web pages and informational directives on o Emergency Preparedness o Hazard Mitigation o Marine Safety o Response and Recovery o A Guide to the Disaster Declaration Process and Federal Disaster Assistance o FEMA's Individual Assistance and Public Assistance programs o A Nuclear Incident Response Team o Customs Role in Countering the Spread of Weapons of Mass Destruction, and o Mitigation Grants programs
Planned Products:	Roadmaps for developing standards for: radiation/nuclear/chemical/biological/cyber-IT countermeasures, and critical infrastructure protection
Additional Information:	Other contacts: 202/282-8000 = Switchboard Bert Coursey 202-772-9536 bert.coursey@dhs.gov
Program Goals:	For the state and local portfolio: 1. Set standards for Homeland Security technology 2. Build mechanisms for analyzing, validating, and setting standards for Homeland Security equipment 3. Develop comprehensive protocols for certification of compliance with these standards

Sectors Addressed:			
☑ ***Law Enforcement***	☐ ***Corrections***	☑ ***EMS***	☐ ***Military***
☐ ***Courts***	☐ ***Probat./Parole***	☑ ***Emerg. Manag.***	☐ ***Other***
☐ ***Public Defender***	☑ ***Fire Protection***	☑ ***Transportation***	
☐ ***Prosecution***	☐ ***Public Works***	☐ ***Utlities***	

Program/Organization:	**SAFECOM Program**
Full Name:	Wireless Public SAFEty Interoperable COMmunications (SAFECOM) Program
Agencies:	Managing Partner - - DHS; OMB e-Gov Initiative
Partnering Agencies / Orgs.:	Numerous local, state, and Federal public safety agencies
Web Page:	http://www.safecomprogram.gov
Contact Name:	David Boyd Program Manager
Contact Phone:	202-772-9531
Contact Email:	david.boyd@dhs.gov or safecom@dhs.gov

Current Products:	o Grant guidance for the communications interoperability lifecycle
Planned Products:	Near-Term Initiatives: o Fully integrate grant guidance across Federal grant programs with interoperable communications funding o Develop and operate an interoperable communications repository on the Web that will allow public safety users to identify the best solutions for their jurisdiction o Develop and promote a national guide and handbook that includes common interoperability terminology for public safety and further addresses communications-related issues to improve the use of Incident Command Systems o Develop fully interoperable demonstrations across the country and create interoperability models out of the successful demonstrations.
Additional Information:	Additional Web site information: www.whitehouse.gov/omb/inforeg/egovstrategy Additional contact: John Cummings, 202-772-9537 john.cummings@dhs.gov
Program Goals:	o Serve as the umbrella program for all public safety communications programs o Ensure that local, tribal, state, and Federal public safety agencies can communicate and share information effectively, efficiently, and across agencies and jurisdictions as they respond to emergency incidents o Reduce decision-making risk in selecting interoperable solutions by identifying solutions based on standards and by developing a common framework for future integration o Reduce loss of life and property due to a lack of public safety communications o Tie guidance to all interoperable wireless communications grants o Develop, implement, and operate a national training and technical assistance program.

Sectors Addressed:	☑ ***Law Enforcement***	☐ ***Corrections***	☑ ***EMS***	☐ ***Military***
	☐ ***Courts***	☐ ***Probat./Parole***	☑ ***Emerg. Manag.***	☐ ***Other***
	☐ ***Public Defender***	☑ ***Fire Protection***	☐ ***Transportation***	
	☐ ***Prosecution***	☐ ***Public Works***	☐ ***Utlities***	

Program/Organization:	**SNSP**
Full Name:	Strategic National Stockpile Program
Agencies:	U.S. Department of Homeland Security, Center for Disease Control and Prevention
Partnering Agencies / Orgs.:	
Web Page:	www.dhs.gov/dhspublic/display?theme=15&content=327
Contact Name:	Timothy R. Bigwood
Contact Phone:	404-639-0625
Contact Email:	ajq3@cdc.gov
Current Products:	o National repository of life-saving pharmaceuticals and medical supplies o Distribution to national emergency site within 12 hours o Support to state and local public health and emergency response officials
Planned Products:	
Additional Information:	www.bt.cdc.gov/stockpile
Program Goals:	o Coordinate with Federal, state, and local emergency responders o Ensure rapid transport of SNS assets in response to terrorism incident

Sectors Addressed:

☐ *Law Enforcement*	☐ *Corrections*	☐ *EMS*	☐ *Military*
☐ *Courts*	☐ *Probat./Parole*	☑ *Emerg. Manag.*	☐ *Other*
☐ *Public Defender*	☐ *Fire Protection*	☐ *Transportation*	
☐ *Prosecution*	☐ *Public Works*	☐ *Utlities*	

Functional Capabilities:

Wireless Voice

☑ Ability of the agency/jurisdiction to administer the priority for voice communications of particular users and particular applications (such as task force operations, incidents, etc.).	We use the Wireless Priority Service along with the Government Emergency Telecommunications System. All services are provided by the NCS.

Wireless Voice

☑ Ability to have secure voice communications.	We use both the STU-III and STE phones. We have the capacity to bring them on deployment if necessary.

Program/Organization:	**SNSP**

Wireless Data

☑ Ability of on-scene personnel to transparently exchange, as authorized, text, image, and/or video data with other on-site personnel, dispatchers, data resources, etc.	We use two-way alphanumeric paging devices.

Wireless Data

☑ Ability to ensure secure exchange of information.	All communications are encrypted. We have a gateway that allows for secure faxes as well.

Wireless Data

☑ Ability to remotely access a user's agency/jurisdiction data communications infrastructure when the user roams outside the radio coverage area of the user's agency/jurisdiction infrastructure.	We have dial-in capability as well as satellite phones that we can use for data as well.

Information Systems

☑ Ability to effectively and efficiently exchange data between agencies/jurisdictions, e.g., by employing common data representation structures and exchange formats and protocols.	We have remote access e-mail capability.

Information Systems

☑ Ability to rapidly access subject information at critical decision points from both field and base locations, including but not limited to information regarding identification (photos, fingerprints, etc.) and activity (criminal history, wants/warrants, reporting/contact history, etc.).	We have a 24/7 Ops center to reach back at the CDC.

Program/Organization:	**TIA**
Full Name:	Telecommunications Industry Association
Agencies:	North American-based SDO
Partnering Agencies / Orgs.:	o Project MESA/ETSI (European Telecommunications Standards Institute) o Project 25 o Industry, Public Safety members and Government participation
Web Page:	http://www.tiaonline.org
Contact Name:	Dan Bart
	Sr. VP, Standards & Special Projects
Contact Phone:	(703) 907-7703
Contact Email:	dbart@tiaonline.org
Current Products:	
Planned Products:	See Project 25 and Project MESA. TIA provides the for a for product development and publication as TIA-only, National, or Regional standards/specifications. Note that TIA TR-45 work involves wireless emergency services.
Additional Information:	
Program Goals:	

BUILDING GLOBAL COMMUNICATIONS

Sectors Addressed:				
☑ ***Law Enforcement***	☑ ***Corrections***	☑ ***EMS***	☑ ***Military***
☐ ***Courts***	☑ ***Probat./Parole***	☑ ***Emerg. Manag.***	☑ ***Other***
☐ ***Public Defender***	☑ ***Fire Protection***	☑ ***Transportation***	***Forestry, Fish & Wildlife, Parks, Natural Resources***
☐ ***Prosecution***	☑ ***Public Works***	☑ ***Utlities***	

Program/Organization:	**TIA TR-8**
Full Name:	Telecommunications Industry Association, TR-8 Mobile and Personal Private Radio Standards
Agencies:	National Association
Partnering Agencies / Orgs.:	SDO'S Government (Federal) Industry
Web Page:	http://www.tiaonline.org
Contact Name:	John Oblak
	Chair, TR-8
Contact Phone:	507-835-6267
Contact Email:	joblak@efjohnson.com
Current Products:	o Land mobile radio, cellular radio standards
Planned Products:	Wideband to Broadband technologies. Multi-jurisdictional and regional interoperability.
Additional Information:	TIA HQ 2500 Wilson Blvd., Suite 300 Arlington, VA 22201 USA ph: (703) 907-7700 John Oblak (EF Johnson) Ph: (507) 835-6267
Program Goals:	o Standards development and promulgation to enhance technologies, gain efficiencies, and promote interoperability o TIA represents providers of communications and information technology products and services for the global marketplace through its core competencies in standards development, domestic and international advocacy, as well as market development and trade promotion programs. The association facilitates the convergence of new communications networks while working for a competitive and innovative market environment. TIA strives to further members' business opportunities, economic growth, and the betterment of humanity through improved communications.

Sectors Addressed:				
☑ ***Law Enforcement***	☑ ***Corrections***	☑ ***EMS***	☑ ***Military***
☐ ***Courts***	☑ ***Probat./Parole***	☑ ***Emerg. Manag.***	☑ ***Other***
☐ ***Public Defender***	☑ ***Fire Protection***	☑ ***Transportation***	***Forestry, Fish & Wildlife, parks, Natural Resources***
☐ ***Prosecution***	☑ ***Public Works***	☑ ***Utlities***	